Núm. Manual		Núm. digital
	B. Documentos Técnicos	2
	C. Propuesta Técnica	3
1	ITEM I. Propuesta Especificaciones Técnicas de las Tarjetas	4
56	ITEM II. Máquinas de Impresión	59
79-1	Entregables Maquinas de Impresión	83
80	ITEM III. Especificaciones técnicas de las PKI CA y PKI Identidad Física y Digital	86
146	ITEM IV. Propuesta Técnica para la Tarjeta de Identidad Digital	152
178-1	ITEM IV. VeriGo MobileID - Anexo Casos de Uso	185
178.22	Componentes Kit Periféricos	206
188	Sección ITEM VI. Parte B. Especificaciones técnicas del Mantenimiento	216
203	ITEM VI. A.1. Instalación de Maquinas de impresión	231
215	ITEM VI. Parte A. Propuesta Infraestructura Centro de Datos	243
242	Sección VII. Capacitación	270
259-1	Datasheet	288
465	Carta de Presentación	517
467-1	Visión del Proyecto	520
470	Curriculum del Líder del Proyecto o Jefe de Proyecto	523
482	Curriculum del Personal Técnico Certificado en Tecnología de impresión de Tarjetas de Identidad	535
499	Curriculum del Personal Técnico en Campo con Experiencia en la Producción de Documentos de Identidad Nacionales	552
586	Certificaciones ISO	639
789-A	Detalle del Cronograma Cumplimiento	842
790	Requisitos de Experiencia (Obligatorios)	849
791	Experiencia en Suministro de Impresoras de Documentos de Identidad de Policarbonato Electrónicos	850
803	Experiencia en Proyecto de Suministro de Tarjetas de Identidad Electrónicas de Policarbonato	862
810	Experiencia en un Proyecto de Suministro de Tarjetas de Identidad Electrónicas de Policarbonato de Transición de Documentos de Identificación Mecánicos (sin electrónica) a documento de identificación electrónicas	869
837	Experiencia en Integración de Sistemas en un proyecto de identificación electrónica	896
844	Requisitos de Experiencia (No Obligatorios)	904
845	Experiencia en Distintos Clientes y Países, en Cedulas Digital o Identidades Móviles (Mobile ID)	905
849	Experiencia de Haber Operado un Proyecto de Impresión de soluciones, al menos doscientas (200) impresoras distribuidas nacional e internacional (fuera del país)	909
852	Experiencia en República Dominicana en proyectos de mantenimiento de tecnología en gobierno con al menos cinco (5) años de experiencia	912
892	Cartas o Declaraciones Juradas	952
908	Plantilla (Matriz)	968

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

EMDOC

B. DOCUMENTOS TECNICOS

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

C. PROPUESTA TÉCNICA

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

ÍTEM I. PROPUESTA ESPECIFICACIONES TÉCNICAS DE LAS TARJETAS

PARA LA CONTRATACIÓN DE LA EMPRESA QUE SE ENCARGARÁ DE SUPLIR LOS EQUIPOS, MATERIALES Y SERVICIOS PARA LA IMPRESIÓN DE LA CÉDULA DE IDENTIDAD Y ELECTORAL (CIE) Y CÉDULA DE IDENTIDAD (CI)

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

EMDOC CONSORCIO

Tabla de contenidos

1 **DOCUMENTOS DE LA TARJETA** 3
1.1 Caracteristicas generales 7
1.2 Tipos de tarjetas 8
1.3 Propuesta de diseño - CIE & CI 8
1.3.1 CIE - Anverso de la tarjeta 8
1.3.2 CIE - Reverso de la tarjeta 9
1.3.3 CIE - Visión general de las funciones de seguridad 10
1.3.4 CI - Anverso de la tarjeta 14
1.3.5 CI - Reverso de la tarjeta 15
1.3.6 CI - Visión general de las funciones de seguridad 16
1.4 Principales medidas de seguridad 20
1.5 Caracteristicas detalladas / Caracteristicas de seguridad de la tarjeta 22
1.5.1 Funciones de seguridad de nivel 1, 2 y 3 22
1.5.2 Otros dispositivos de seguridad 23
1.5.3 Resistencia de la tarjeta según la OACI 24
1.5.4 Glosario de elementos de seguridad 25
1.5.5 Caracteristicas electrónicas y sistema operativo 33
1.5.5.1 Caracteristicas del chip sin contacto 33
1.5.5.2 Caracteristicas del sistema operativo 34
1.6 Tarjeta de muestra 36
1.6.1 Vista previa 36
1.6.1.1 Parte delantera 36
1.6.1.2 Parte trasera 36
1.6.2 Descripción general de las funciones de seguridad 38
1.7 Matriz de conformidad 42
1.8 Embalaje y transporte 44
1.9 Entregables 45
1.10 Derechos de propiedad 46
1.11 Control de calidad 46
2 **TÉRMINOS DE REFERENCIA** 47
2.1 Punto I: Especificaciones técnicas de las tarjetas 47

EMDOC CONSORCIO

1 Documentos de la tarjeta

A continuación se describe la propuesta de tarjetas de identidad en blanco de este tipo:

- Tarjeta de Identidad y Electoral (CIE) y
- Documento de identidad (CI).

Las tarjetas propuestas son sin contacto (con Documento Electrónico de Viaje. Firma electrónica y funcionalidad de identificación del ciudadano) y están fabricados con materiales de policarbonato que se fusionan a alta temperatura y pueden personalizarse de forma óptima mediante un proceso de grabado por láser. Esta combinación de material de policarbonato y método de personalización por grabado láser proporciona unas características excepcionales del documento en términos de durabilidad y seguridad. Un amplio conjunto de elementos de seguridad ayudará a proteger la tarjeta contra la falsificación.



Centro de producción principal y centro de producción de reserva

La producción de la tarjeta corre a cargo del socio del consorcio Mühlbauer ID Services GmbH. Mühlbauer cuenta con dos plantas de producción de tarjetas en Roding (Alemania) y Stara Pasova (Serbia), que están igualmente equipadas en cuanto a sistemas de maquinaria y capacidad de producción. Desde la perspectiva actual, la planta de Roding está prevista para la producción de las tarjetas propuestas.

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.



Planta principal de producción en la sede de Mühlbauer, Roding, Alemania



Planta de producción de reserva en Mühlbauer Stara Pazova, Serbia

Gracias a sus equipos técnicos y capacidades de producción equivalentes, ambos centros pueden asegurar un alto nivel de disponibilidad de la producción y garantizar así la continuidad de la actividad.

Certificaciones
Ambos centros de producción están certificados para la producción de documentos de seguridad de acuerdo con las normas aplicables, como:

- ISO 9001:2015
- ISO 27001:2013
- ISO 14001
- ISO 14298 INTERGRAF

CONSORCIO EMDOC EMDOC CONSORCIO 4 Santo Domingo, R.D.



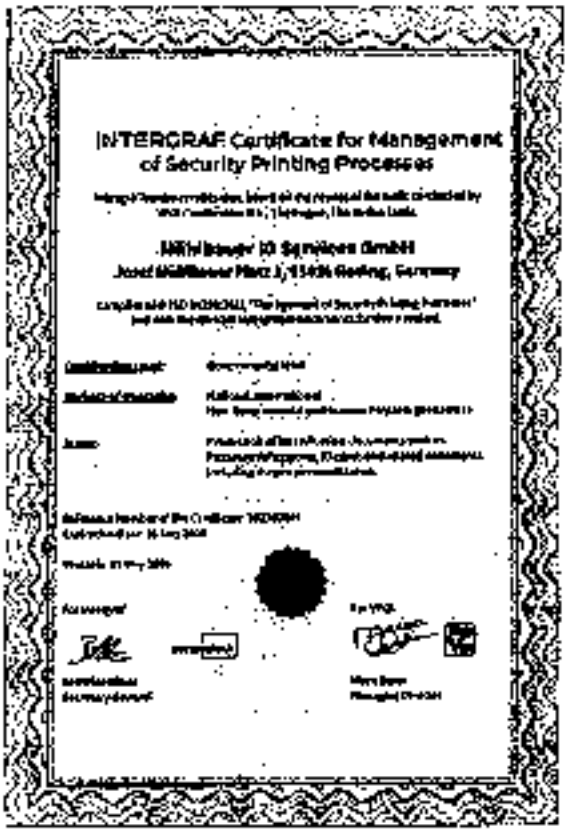
Los procesos generales de Mühlbauers, que cumplen la norma **ISO 9001**, garantizarán la participación de toda la organización en el aseguramiento de la calidad de los productos y servicios que se proporcionarán a la JCE.

La serie **ISO/IEC 27001** es un conjunto de normas que proporcionan un marco de gestión de la seguridad de la información (método, documentación, definición de objetivos y evaluación de riesgos).

CONSORCIO EMDOC
EMDOC
CONSORCIO
5
Santo Domingo, R.D.

EMDOC CONSORCIO





ISO 14001, que establece que se ha implantado un sistema de gestión medioambiental para mejorar el comportamiento medioambiental, cumplir las obligaciones legales y de otro tipo y alcanzar los objetivos medioambientales.

ISO 14298, que establece los requisitos mínimos de un sistema de gestión de la seguridad de la impresión.

iotek Mühlbauer GSI ULTRATECH VERIDOS

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

1.1 Características generales

Basándonos en los requisitos de la licitación y en nuestros conocimientos y experiencia, las especificaciones técnicas se describen en formato ID1 según la norma ISO 7810. El diseño del fondo de seguridad se creará con un software especial de diseño de seguridad y se imprimirá con impresión offset de alta resolución, como se hace en los documentos de seguridad.

Los documentos de identidad propuestos tendrán las dimensiones y tolerancias especificadas por:

- ISO/IEC 7816:2019
- ISO/IEC 7810:2019
- OACI 9303/2021
- La tarjeta sin contacto cumplirá las actuales normas ISO/IEC 14443.

Característica	Descripción
Materiales para tarjetas	• 100% Policarbonato o formado por varias capas (5 como mínimo) o fusionados mediante laminación resistente a la rotura en caliente • Tintas conformes a la norma de durabilidad ISO 18745 y solidez a la luz de 4 en la escala de lana azul o formulaciones de tinta específicas para sistemas de impresión offset o tintas de seguridad de pigmentos sólidos o Tintas ópticas variables
De por vida	Vida útil mínima de 10 años en condiciones de uso normal
Construcción de tarjetas	• Construcción multicapa de alta seguridad sin ningún tipo de pegamento • Mínimo 5 capas • La construcción del cuerpo de la tarjeta se ha diseñado sin capas ni materiales patentados que limiten la obtención de materiales para la producción de tarjetas de proveedores especializados. • El cuerpo de la tarjeta en blanco y el proceso de personalización de tarjetas en combinación no constituirán una solución dependiente o patentada que excluya a los proveedores de tarjetas y/o sistemas de personalización • Elemento holográfico en el anverso (protección del retrato) y elemento OVD en el reverso (impresión iridiscente) que protege el retrato por el reverso
Dimensiones de la tarjeta en blanco	• Según la norma ISO 7810 (ID1) Medidas / Mínimo / Máximo Espesor / 0,68 mm / 0,84 mm Anchura / 85,47 mm / 85,72 mm Altura / 53,92 mm / 54,03 mm
Tecnología de personalización	• Grabado láser de alta resolución de datos personales (escala de grises)
Tecnología de chips	• Chip sin contacto conforme a la norma ISO/IEC 14443

CONSORCIO EMDOC Cr EMDOC CONSORCIO Santo Domingo, R.D.

1.2 Tipos de tarjetas

El Consorcio EMDOC entregará dos tipos de tarjetas:

- Tarjeta de Identidad y Electoral (CIE) y
- Documento de Identidad (CI).

Las tarjetas tendrán las mismas características físicas estipuladas, variando únicamente en cuanto al color de la tarjeta (fondos preimpresos) y su personalización en el reverso.

Las tarjetas tendrán:

- Diseño exclusivo de los fondos de seguridad impresos en offset, contemplando guilloches, microtextos combinados con motivos o imágenes alegóricas a la República Dominicana, constituidos por líneas finas continuas con modulación de su grosor u otros patrones de alta seguridad, motivos impresos en al menos dos colores de tinta visible, que serán fluorescentes en el anverso al menos cuando se expongan a una fuente de luz ultravioleta.
- Estampado de superficies en relieve mediante laminación en registro.
- Estructura lenticular para poder personalizar una CLI o ML1.
- La ventana transparente

1.3 Propuesta de diseño - CIE & CI

El diseño que figura a continuación incluye los elementos de seguridad solicitados y propuestos y debe entenderse como una perspectiva de un posible enfoque de diseño. El diseño final se coordinará con JCE y todos los archivos de diseño se entregarán en archivos vectoriales en formato electrónico. JCE poseerá todos los derechos de los diseños proporcionados.

1.3.1 CIE - Anverso de la tarjeta



Vista previa del diseño de la tarjeta en blanco con luz normal



Vista previa del diseño de la tarjeta personalizada con luz normal

CONSORCIO EMDOC EMDOC CONSORCIO B Santo Domingo, R.D.

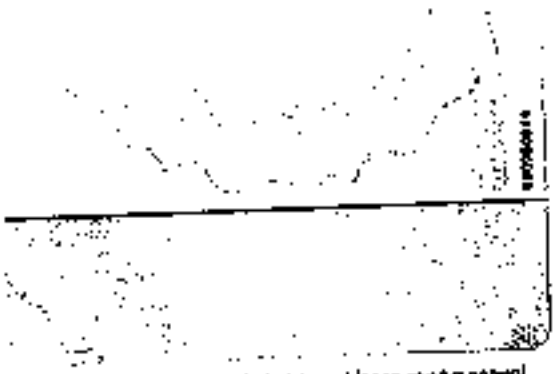


Vista previa del diseño de la tarjeta en blanco bajo luz ultravioleta



Vista previa del diseño de la tarjeta en blanco bajo luz IR

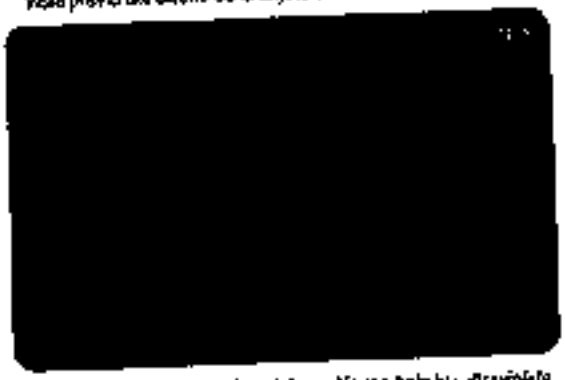
1.3.2 CIE - Reverso de la tarjeta



Vista previa del diseño de la tarjeta en blanco con luz normal



Vista previa del diseño de la tarjeta personalizada con luz normal



Vista previa del diseño de la tarjeta en blanco bajo luz ultravioleta

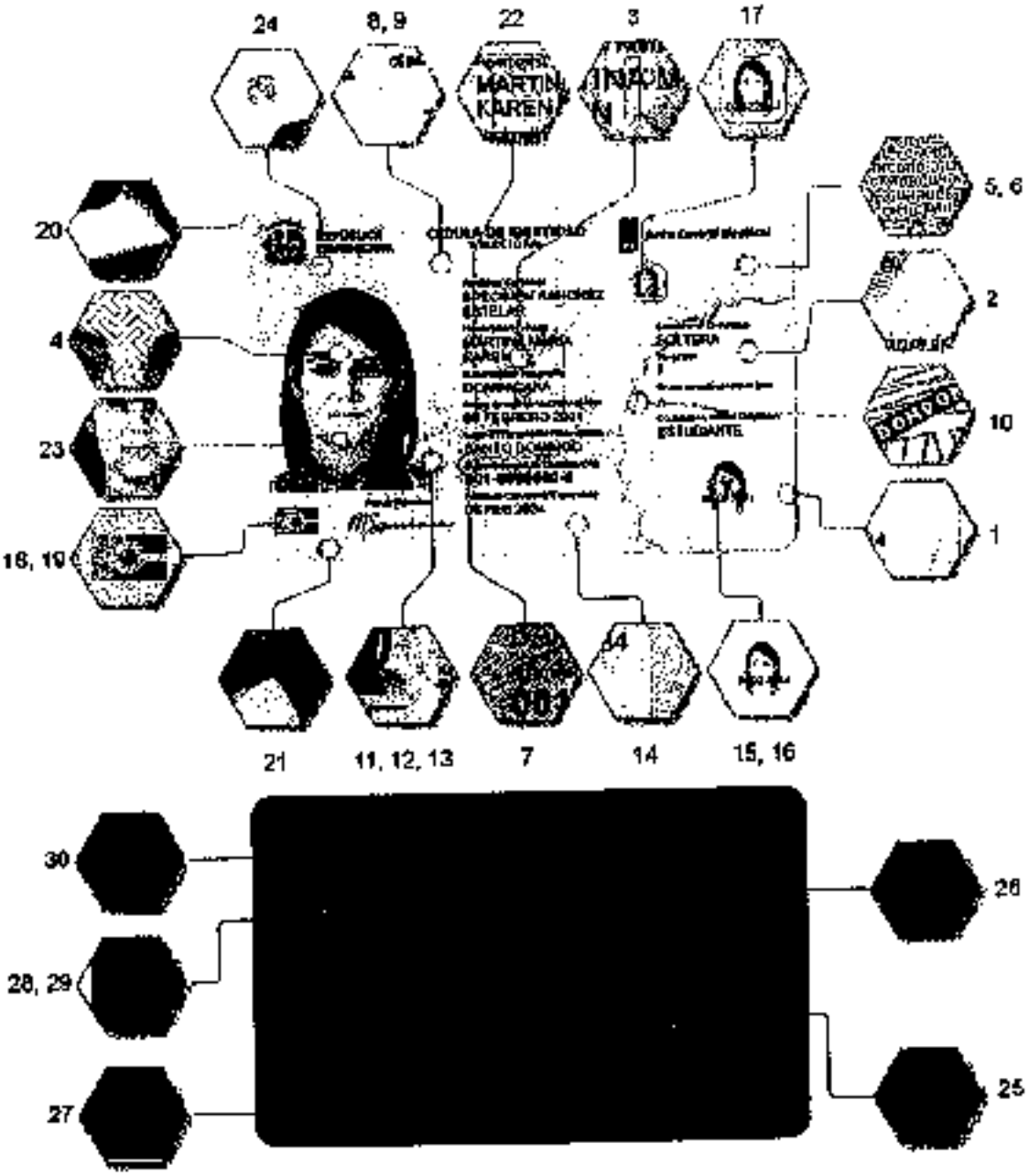


Vista previa del diseño de la tarjeta en blanco bajo luz IR

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

EMDOC CONSORCIO

1.3.3 CIE - Visión general de las funciones de seguridad

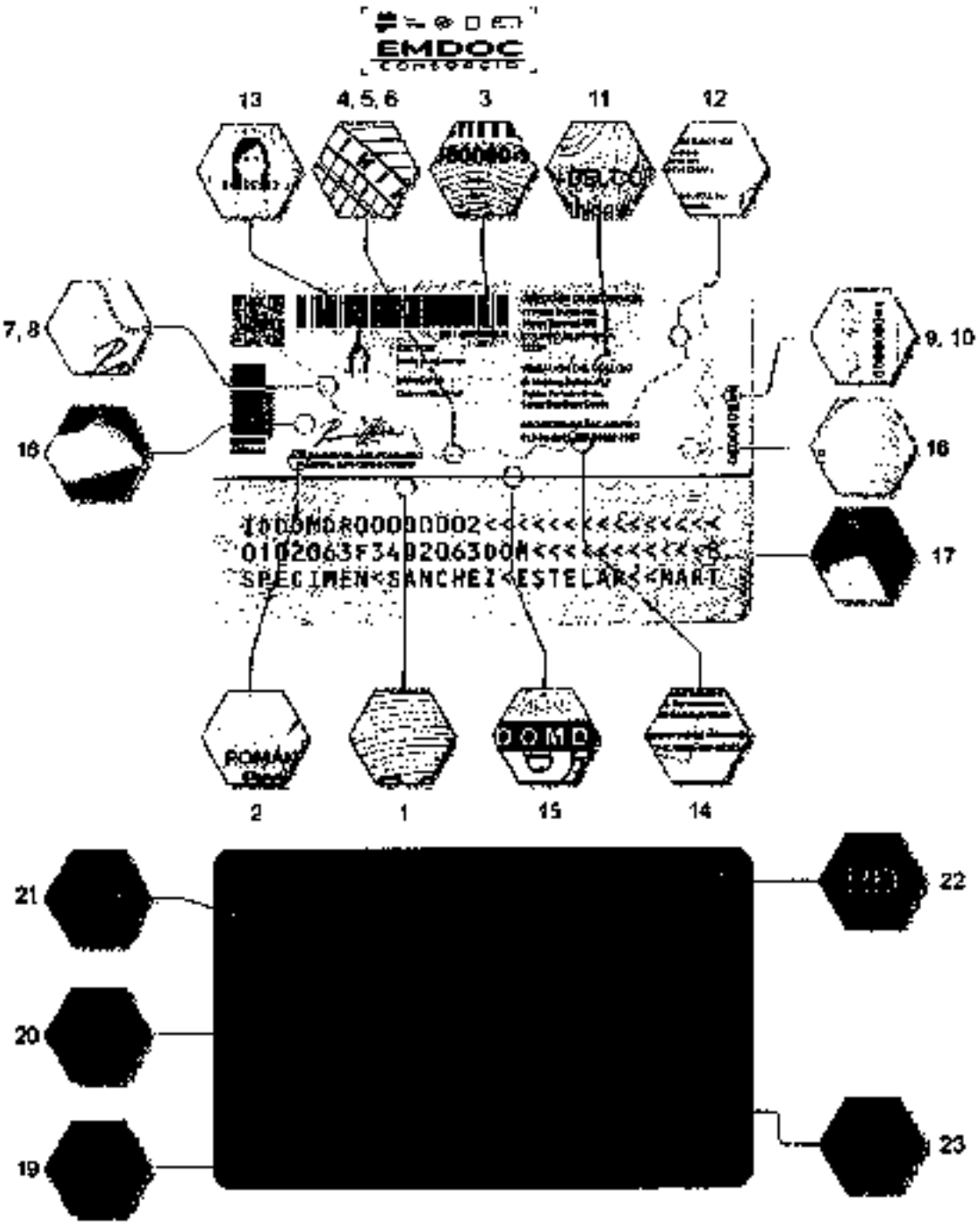


CONSORCIO EMDOC EMDOC CONSORCIO 10 Santo Domingo, R.D.

EMDOC

No.	Elemento de seguridad	No.	Elemento de seguridad
1	Guilloches	16	Estructura lenticular (CLI)
2	Guilloches negativos	17	Ventana transparente (que contiene la imagen del titular y la fecha de caducidad)
3	Diseño 3D (numismático)	18	Tinta Óptica Variable (OVI)
4	Pantalla fractal	19	Tinta luminiscente infrarroja (efecto antistokes)
5	Leyenda de microtexto repetitiva (pantalla de microtexto)	20	Construcción multicapa (mínimo 5 capas)
6	Microtexto positivo	21	Tintas de seguridad mixtas exclusivas
7	Tipo de letra no estándar para texto desplazado	22	Grabado láser táctil
8	Impresión arco iris (Iris)	23	Fondo de seguridad fusionado con el área de retrato (Protección de retrato)
9	Pantalla de arte (Art screen)	24	Tintas invisibles en IR
10	Microtexto negativo incl. falta de ortografía deliberada	25	Material mate UV
11	Elemento óptico difractivo variable (parcialmente superpuesto Retrato del titular)	26	Microtexto fluorescente UV
12	Microtexto en el interior de un elemento óptico difractivo variable	27	Impresión arco iris fluorescente UV
13	Nanotexto en el interior de un elemento óptico difractivo variable	28	Diseño fluorescente UV en la zona del retrato
14	Elemento táctil (relieve superficial) en alto relieve	29	Fondo de seguridad invisible
15	Imagen secundaria (imagen fantasma)	30	Pigmentos fluorescentes UV incorporados en tinta visible

CONSORCIO EMDOC EMDOC CONSORCIO 11 Santo Domingo, R.D.



CONSORCIO EMDOC
EMDOC
CONSORCIO
12
Santo Domingo, RD

EMDOC

No.	Elemento de seguridad	No.	Elemento de seguridad
1	Modulación de anchura de línea	13	Ventana transparente
2	Pantalla de arte	14	Grabado por láser de datos personales
3	Diseño dúplex	15	Microtexto negativo
4	Microtexto positivo	16	Construcción multicapa (mínimo 5 capas)
5	Error ortográfico deliberado	17	Tintas de seguridad mixtas exclusivas
6	Microtexto de tamaño variable	18	Elemento OVD (tinta iridiscente)
7	Seguridad	19	Material mate UV
8	Impresión arco iris (Iris)	20	Impresión arco iris fluorescente UV
9	Número de cuerpo de tarjeta único prepersonalizado grabado con láser	21	Malla de microtexto de fondo fluorescente UV
10	Grabado láser táctil	22	Impresión UV bi-fluorescente
11	Guilloches	23	Pigmentos fluorescentes UV incorporados en tinta visible
12	Tintas invisibles en IR		

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

EMDOC CONSORCIO

1.3.4 CI - Anverso de la tarjeta



Vista previa del diseño de la tarjeta en blanco con luz normal



Vista previa del diseño de la tarjeta personalizada con luz normal



Vista previa del diseño de la tarjeta en blanco bajo luz ultravioleta

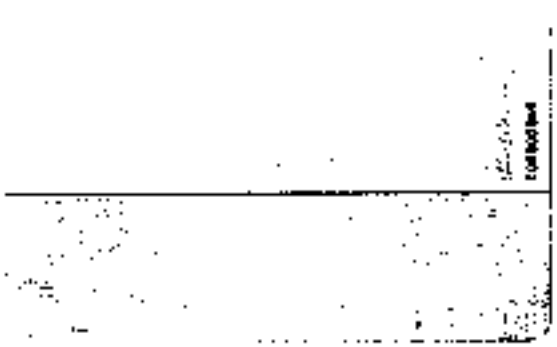


Vista previa del diseño de la tarjeta en blanco bajo luz IR

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

EMDOC CONSORCIO

1.3.5 CI - Reverso de la tarjeta



Vista previa del diseño de la tarjeta en blanco con luz normal



Vista previa del diseño de la tarjeta personalizada con luz normal



Vista previa del diseño de la tarjeta en blanco bajo luz ultravioleta

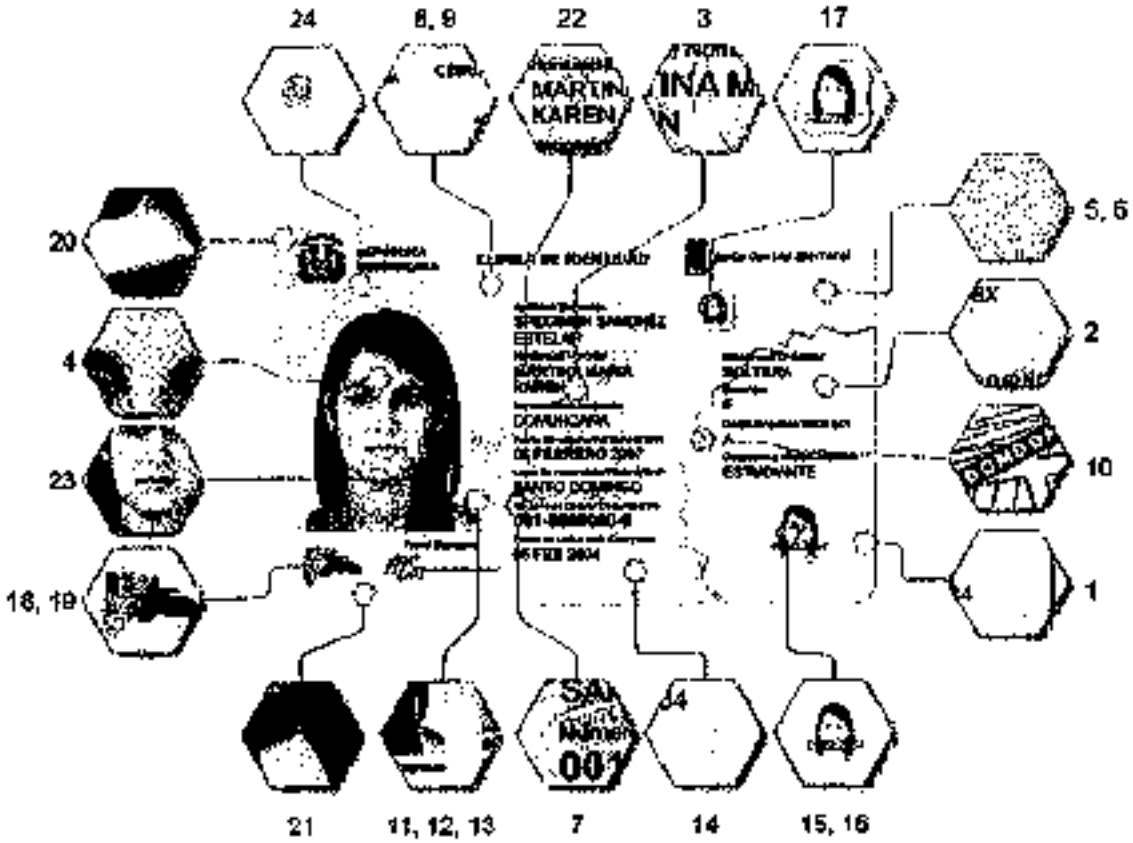


Vista previa del diseño de la tarjeta en blanco bajo luz IR

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

EMDOC CONSORCIO

1.3.6 CI - Visión general de las funciones de seguridad



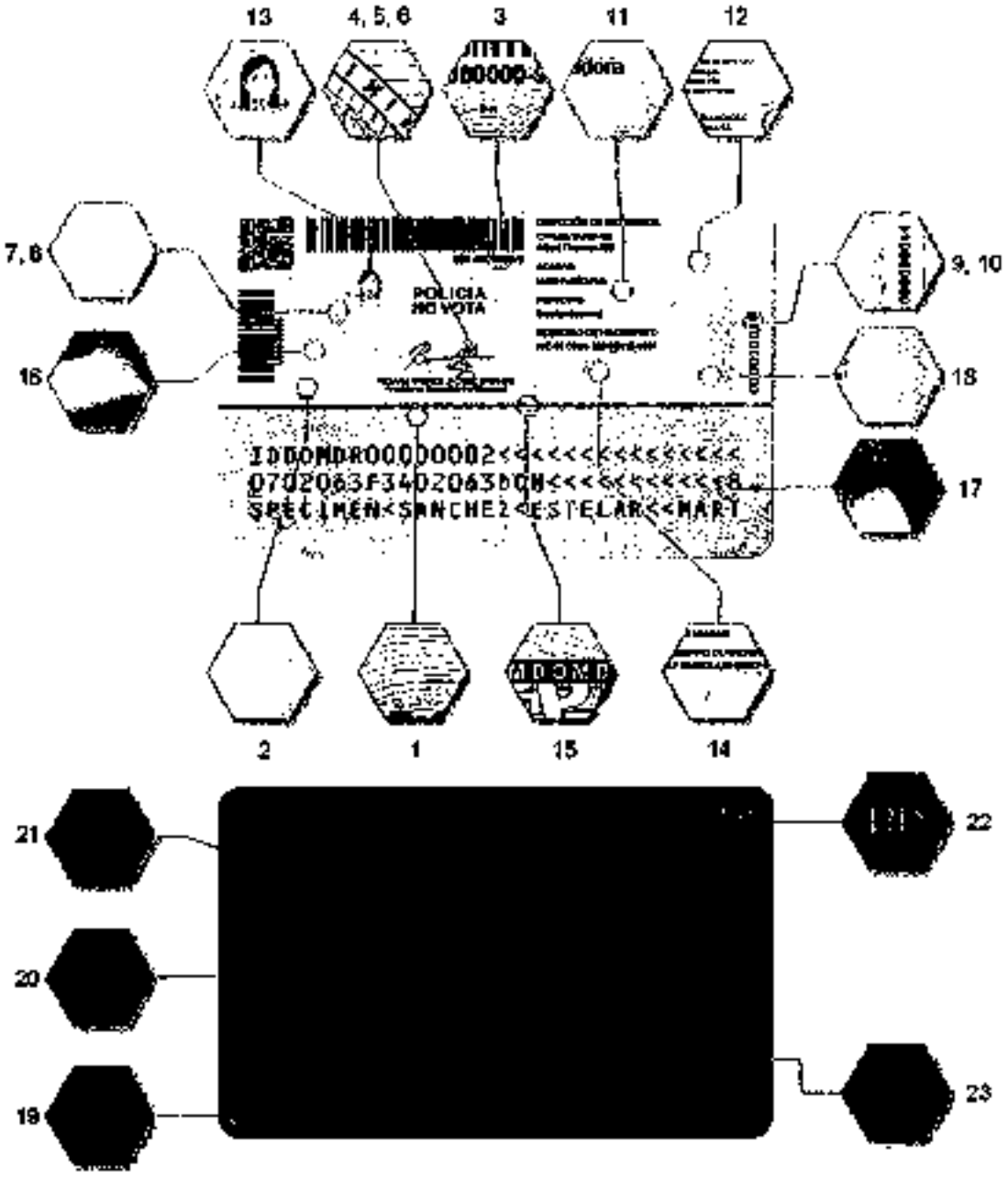


EMDOC
CONSORCIO

No.	Elemento de seguridad	No.	Elemento de seguridad
1	Guilloches	16	Estructura lenticular (CLI
2	Guilloches negativos	17	Ventana transparente (que contiene la imagen del titular y la fecha de caducidad)
3	Diseño 3D (numismático)	18	Tinta Óptica Variable (OVI)
4	Pantalla fractal	19	Tinte luminiscente infrarroja (efecto antistokes)
5	Leyenda de microtexto repetitive (pantalla de microtexto)	20	Construcción multicapa (mínimo 5 capas)
6	Microtexto positivo	21	Tintas de seguridad mixtas exclusivas
7	Tipo de letra no estándar para texto desplazado	22	Grabado láser táctil
8	Impresión arco iris (Iris)	23	Fondo de seguridad fusionado con el área de retrato (Protección de retrato)
9	Pantalla de arte	24	Tintas invisibles en IR
10	Microtexto negativo ind. falla de ortografía deliberada	25	Material mate UV
11	Elemento óptico difractivo variable (parcialmente superpuesto Retrato del titular)	26	Microtexto fluorescente UV
12	Microtexto en el interior de un elemento óptico difractivo variable	27	Impresión arco iris fluorescente UV
13	Nanotexto en el interior de un elemento óptico difractivo variable	28	Diseño fluorescente UV en la zona del retrato
14	Elemento táctil (relieve superficial) en altorrelieve	29	Fondo de seguridad invisible
15	Imagen secundaria (imagen fantasma)	30	Pigmentos fluorescentes UV incorporados en tinta visible

CONSORCIO EMDOC EMDOC CONSORCIO 17 Santo Domingo, R.D.

EMDOC
CONSORCIO



CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

iOtek cit Mühlbauer GSI ULTRATECH VERIDOS

EMDOC
CONSORCIO

No.	Elemento de seguridad	No.	Elemento de seguridad
1	Modulación de anchura de línea	13	Ventana transparente
2	Pantalla de arte	14	Grabado por láser de datos personales
3	Diseño dúplex	15	Microtexto negativo
4	Microtexto positivo	16	Construcción multicapa (mínimo 5 capas)
5	Error ortográfico deliberado	17	Tintas de seguridad mixtas exclusivas
6	Microtexto de tamaño variable	18	Elemento OVD (tinta iridiscente)
7	Seguridad	19	Material mate UV
8	Impresión arco iris (Iris)	20	Impresión arco iris fluorescente UV
9	Número de cuerpo de tarjeta único prepersonalizado grabado con láser	21	Malla de microtexto de fondo fluorescente UV
10	Grabado láser táctil	22	Impresión UV bi-fluorescente
11	Guilloches	23	Pigmentos fluorescentes UV incorporados en tinta visible
12	Tintas invisibles en IR		

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.
19

EMDOC CONSORCIO

1.4 Principales medidas de seguridad

Suministro de dibujos y modelos en formato electrónico y cesión de propiedad
Como se exige en el pliego de condiciones, el diseño acordado se entrega a la JCE en formato electrónico como archivos vectoriales. La propiedad se transfiere a la JCE.

Características del diseño de la tarjeta
Además, se confirma que el diseño final acordado incluirá, en consonancia con la viabilidad técnica evaluada por la JCE, los siguientes aspectos:

- un diseño creado exclusivamente para la JCE, que incluye fondos de seguridad para ser impresos en offset, guilloches inklusivos, microtext combinados con motivos o imágenes alegóricas a la República Dominicana hechos de líneas finas continuas con modulación de su delgadez.
- un diseño impreso en al menos dos (2) colores de tinta visibles que muestra fluorescencia en el reverso al menos cuando se expone a una fuente de luz ultravioleta
- una superficie estampada en relieve mediante laminación en registro
- una estructura lenticular para un CLI o un MLI
- una ventana transparente de forma y posición definidas en la tarjeta

Sobre el sistema de personalización

También se ha confirmado que el cuerpo de la tarjeta propuesta permitirá un proceso de grabado por láser para personalizarla:

- Datos variables
- Imágenes (imagen principal, imágenes secundarias)
- Funciones de seguridad (CLI o MLI, otras)

Grabado por láser de texto y grabado de imágenes



Grabado por láser de grabado MLI o CLI

CONSORCIO EMDOC EMDOC CONSORCIO 20 Santo Domingo, R.D.

EMDOC
CONSORCIO



La estación láser del sistema de la máquina de personalización está equipada con una unidad giratoria para grabar la Imagen Láser Múltiple (MLI) de seguridad o una Imagen Láser Cambiable (CLI).



EMDOC CONSORCIO

1.5 Caracteristicas detalladas / Caracteristicas de seguridad de la tarjeta

1.5.1 Funciones de seguridad de nivel 1, 2 y 3

Característica	Descripción	
	• Impresión arco iris (Ins) • Guilloches • Guilloches negativos • Tinta variable óptica (IR visible) • Diseño 3D (numismático) • Pantalla fractal • Modulación de anchura de línea • Pantalla de arte • Diseño dúplex • Elemento óptico difractivo variable (parcialmente superpuesto Retrato del titular) • Elemento OVD (impresión iridiscente)	• Elementos táctiles (relieve superficial) en altorrelieve en el anverso de la tarjeta • Seguridad • Fondo de seguridad fusionado con el área de retrato (Protección de retrato) • Imagen de titulares secundarios (imagen fantasma) • Número de cuerpo de tarjeta único prepersonalizado grabado con láser • Estructura lenticular (MLI/ CLI) • Grabado láser táctil • Grabado por láser de datos personales • Ventana transparente
	• Elementos de microtexto en el anverso y reverso de la tarjeta • Microtexto negativo, tanto en el anverso como en el reverso de la tarjeta • Falta de ortografía deliberada dentro de un microtexto • Microtexto en el interior de óptico difractivo variable • Leyenda de microtexto repetitive (pantalla de microtexto) • Tipo de letra no estándar para texto desplazado	• Microtexto de tamaño variable • Material mate UV • Microtexto fluorescente UV • Malla de microtexto de fondo fluorescente UV • Impresión arco iris fluorescente UV • Diseño fluorescente UV en la zona del retrato • Impresión UV bi-fluorescente • Pigmentos fluorescentes UV incorporados en tinta visible
	• Nanotexto en el interior de óptico difractivo variable • Fondo de seguridad visible e invisible en la zona del retrato • Tintas de seguridad mixtas exclusivas	• Construcción multicapa (mínimo 5 capas) • Tintas invisibles en IR • Tinta luminiscente infrarroja (efecto antistokes)

CONSORCIO EMDOC EMDOC CONSORCIO 22 Santo Domingo, R.D.

EMDOC CONSORCIO

1.5.2 Otros dispositivos de seguridad

Las tarjetas contendrán los siguientes elementos de seguridad. La implantación de la incrustación en el diseño general se coordinará con la JCE en función de la viabilidad técnica.

Pos.	Descripción	Método de inspección
1	**ELEMENTO ÓPTICO DIFRACTIVO VARIABLE** Los hologramas son dispositivos de seguridad que contienen una amplia game de elementos de seguridad adicionales, como microtexto, nanotexto, colores espectrales, guillochés, efectos tridimensionales o elementos holográficos especiales. Dependiendo de la iluminación o del ángulo de visión, el aspecto de los hologramas cambia en cuanto a color y diseño. El hecho de que el holograma esté protegido por numerosas capas inseparablemente laminadas dificulta enormemente la manipulación del documento sin dañar visiblemente su estructura.	Esta función de seguridad puede verificarse sin utilizar dispositivos adicionales cambiando la iluminación y/o la dirección de visión.
2	**ELEMENTOS TÁCTILES (ESTRUCTURA EN RELIEVE DE LA SUPERFICIE TÁCTIL)** Esta estructura en relieve sobre la superficie del documento se aplica durante la producción del documento utilizando planchas de laminación grabadas especiales. El relieve consiste en líneas perceptibles u otros elementos de diseño, que aparecen en relieve positivo, negativo o mate en la superficie de los documentos. El preciso proceso de fabricación permite incluso integrar elementos de seguridad adicionales, como una imagen latente o un microtexto. Los intentos de separar las capas del documento o de reproducirlo en su totalidad serán reconocidos inmediatamente, ya que la superficie gofrada del documento quedará visiblemente dañada en cualquier caso.	Este dispositivo de seguridad puede verificarse sin utilizar dispositivos adicionales cambiando la iluminación y/o la dirección de visión. También se puede detectar hápticamente.
3	**VENTANA TRANSPARENTE** La ventana transparente es un área definida del documento que es transparente. Está hecha de polímero y puede incluir opcionalmente otros elementos de seguridad o datos personalizados. Como la Ventana Transparente se produce durante un sofisticado proceso de fabricación y se incrusta en el cuerpo del documento, es muy difícil reproducirla sin dañar notablemente la estructura del documento.	Esta función de seguridad puede verificarse sin utilizar dispositivos adicionales mediante el ojo humano.
4	**ESTRUCTURA LENTICULAR - IMAGEN LÁSER MÚLTIPLE (MLI)IMAGEN LÁSER CAMBIANTE (CLI)** La tecnología MLI/ CLI es un elemento de seguridad ópticamente variable personalizado. Ya durante el proceso de producción, se graba en la superficie del documento un conjunto de lentes cilíndricas. Estas lentes contienen el MLI/ CLI, que se personaliza mediante grabado láser y puede contener información específica del titular (por ejemplo, retrato del titular, fecha de nacimiento, número personal). Dado que el MLI/ CLI está grabado en varias capas del cuerpo del documento, es detectable	Esta función de seguridad puede verificarse sin ningún dispositivo adicional. Cambiando el ángulo de visión se puede ver información diferente dentro de la lente.

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D. 23

	forzosamente durante un análisis de laboratorio. Dado que la inclusión de un MLI/ CLI en un documento de seguridad requiere mucha experiencia y conocimientos técnicos (por ejemplo, en términos de ángulos de las lentes, ajustes del láser, etc.), es extremadamente difícil falsificarlo o imitarlo.	
5	**PROTECCIÓN DEL RETRATO DEL PROPIETARIO** El fondo de seguridad impreso en offset (visible e invisible) se superpone y fusiona con la zona del retrato sin interferir en la correcta visualización y, por tanto, ofrece una protección adicional contra la sustitución de la fotografía del titular y la alteración de los datos del documento de identificación. Además, el retrato del titular quedará protegido al superponerse sobre él el elemento óptico difractivo.El hecho de que el holograma esté protegido por numerosas capas inseparablemente laminadas dificulta enormemente la manipulación del documento sin dañar visiblemente su estructura.	La característica de seguridad visible puede ser verificada por el ojo humano y la característica de seguridad invisible puede ser verificada iluminando el documento con luz ultravioleta (365 nm).
6	**NÚMERO DE TARJETA PREPERSONALIZADO GRABADO CON LÁSER** Durante el proceso de fabricación, se aplica un número único al documento en blanco. Este número permite el seguimiento preciso de cada documento durante toda la cadena de producción y la gestión de todo el ciclo de vida. Gracias al número único, los documentos robados pueden identificarse sin problemas e invalidarse para evitar que se sigan utilizando indebidamente.	Esta función de seguridad puede verificarse sin utilizar dispositivos adicionales mediante el ojo humano.

1.5.3 Resistencia de la tarjeta según la OACI

Junto con el primer lote de tarjetas, Mühlbauer entregará informes de pruebas de laboratorios independientes certificados para:

- **Durabilidad:** La durabilidad del soporte estará garantizada por un periodo de 10 años.
- **Deformación:** La deformación causada por el uso normal es tal que puede enderezarse con el equipo de lectura sin afectar al uso de la tarjeta ni a su funcionamiento.
- **Toxicidad:** No debería presentar ningún riesgo tóxico en condiciones normales de uso.
- **Resistencia a los productos químicos:** Será resistente a los efectos químicos inherentes a su manipulación y uso normal, excepto cuando se le haya dotado de sensibilidad química por razones de seguridad.
- **Estabilidad térmica:** Seguirá siendo legible mecánicamente a temperaturas comprendidas entre -10 °C y +50 °C. La tarjeta no perderá su funcionalidad si se expone a temperaturas que oscilen entre -35 °C y +80 °C.
- **Humedad:** La tarjeta será legible por la máquina con una humedad relativa ambiente del 5% al 95% y una temperatura máxima de bulbo húmedo de 25°C. La tarjeta no perderá su funcionalidad si se almacena o se expone a una humedad relativa ambiente del 0% al 100% (sin condensación).

EMDOC CONSORCIO Santo Domingo, RD

1.5.4 Glosario de elementos de seguridad

La elección del sustrato adecuado es una de las partes más importantes de la producción de documentos de alta seguridad. Durante el proceso de producción, el sustrato puede modificarse con elementos de seguridad adicionales. El uso de sustratos de alta seguridad no sólo impide la falsificación y la imitación, sino que también garantiza la mejor calidad y vida útil posibles de los documentos de identidad.

Pos.	Descripción	Método de inspección
1	**TINTA ÓPTICA VARIABLE (OVMI)** En cuanto cambia el ángulo de visión, los elementos de tinta variable óptica cambian entre dos colores diferentes. Conocidas por la impresión de billetes y otros documentos de seguridad, estas tintas ópticas variables sólo se suministran a imprentas certificadas de alta seguridad. Como el efecto de cambio de color de la tinta no puede copiarse ni imitarse, cualquier intento de falsificación del documento será inmediatamente visible.	Esta función de seguridad puede verificarse sin ningún dispositivo adicional. Sólo cambiando el ángulo de visión se pueden ver colores diferentes.
2	**IMPRESIÓN ARCO IRIS** La impresión arco iris es una de las tecnologías de impresión de seguridad más antiguas, pero todavía más eficaces y probadas. Una separación de colores del diseño de fondo se imprime en la misma unidad de impresión en dos colores (A-B-A) o tres colores (A-B-C). De forma similar a un arco iris en el cielo, los distintos colores se funden a la perfección sin dejar espacios entre ellos. Este cambio continuo de color no puede copiarse sin un efecto de tramado claramente visible. Por tanto, este proceso de impresión de alta seguridad protege el documento contra imitaciones y falsificaciones.	Esta característica de seguridad puede verificarse sin utilizar dispositivos adicionales mediante el ojo humano. Además, utilizando un dispositivo de aumento se puede ver una transición de color suave.
3	**GUILLOCHES** Los guilloches son objetos personalizados, continuos, normalmente de líneas finas (líneas simples o rosetas), que siguen una apariencia tradicional. Impresos con uno o varios colores, pueden formar parte del objeto de diseño de fondo o constituir por sí mismos un elemento de diseño. Controlado mediante fórmulas matemáticas, el aspecto de los guilloches es único; de este modo, el diseño del documento es difícil de imitar y la imagen facial del portador del documento queda protegida contra la sustitución. La seguridad del guilloche puede aumentarse mejorando el patrón del guilloche hasta convertirlo en una representación tridimensional. Además, esta función de seguridad de última generación puede combinarse con el patrón dúplex y la modulación del ancho de línea.	Esta característica de seguridad puede verificarse sin utilizar dispositivos adicionales mediante el ojo humano. Además, utilizando un dispositivo de aumento se puede ver una transición.

CONSORCIO EMDOC EMDOC CONSORCIO 25 Santo Domingo, R.D.

EMDOC

4	**DISEÑO 3D (NUMISMÁTICO)** En general, los objetos en relieve consisten en una compleja red de líneas finas que forman una impresión tridimensional de elementos de texto, logotipos o elementos gráficos. Este elemento de seguridad puede validarse simplemente a simple vista o mediante una lupa. Al igual que un patrón antiescáner, el relieve de diseño tridimensional tiene un efecto antiocopia. Además, debido a su compleja estructura, el relieve de diseño tridimensional es muy difícil de imitar.	Esta característica de seguridad puede verificarse sin utilizar dispositivos adicionales mediante el ojo humano. Además, utilizando un dispositivo de aumento se puede ver una transición.
5	**FONDO DE SEGURIDAD FUSIONADO CON EL ÁREA DE RETRATO** El fondo de seguridad impreso en offset se superpone y fusiona con la zona del retrato sin interferir en la correcta visualización y, por tanto, ofrece una protección adicional contra la sustitución de la fotografía del titular y la alteración de los datos del documento de identificación.	Esta función de seguridad puede verificarse sin utilizar dispositivos adicionales mediante el ojo humano.
6	**MICROTEXTO NEGATIVO (INCLUIDA LA FALTA DE ORTOGRAFÍA DELIBERADA)** El microtexto negativo sigue las mismas reglas que el microtexto impreso normal y consiste en letras pequeñas, apenas perceptibles a simple vista, pero que se hacen visibles con una ampliación. El microtexto negativo no se imprime en forma de letras, sino omitiendo deliberadamente el diseño de color circundante, creando una imagen negativa de letras que aparecen como texto blanco.	Estos elementos de seguridad pueden verificarse mediante inspección con lupa.
7	**MICROTEXTO POSITIVO (INCLUIDA LA FALTA DE ORTOGRAFÍA DELIBERADA)** Los microtextos son letras o números impresos muy pequeños, apenas perceptibles a simple vista, pero que se hacen visibles con una ampliación. Son un elemento de seguridad elemental y una parte esencial del concepto de seguridad de los documentos de identidad.	Estos elementos de seguridad pueden verificarse mediante inspección con lupa
8	**MODULACIÓN DE ANCHURA DE LÍNEA** Este elemento de seguridad se caracteriza porque la anchura de las líneas cambia continuamente. Esta técnica puede emplearse para mejorar la seguridad de numerosos elementos de diseño (por ejemplo, guilloches o fractales), así como para añadir un efecto tonal a pantallas o relieves tridimensionales. Como estas líneas de anchura modulada son difíciles de rediseñar o reproducir, contribuyen significativamente a aumentar la protección contra falsificaciones del documento.	Esta característica de seguridad puede verificarse sin utilizar dispositivos adicionales mediante el ojo humano. Además, utilizando un dispositivo de aumento se puede ver una transición.

CONSORCIO EMDOC
EMDOC CONSORCIO
Santo Domingo, RD

EMDOC CONSORCIO

9	**ANTECEDENTES DE SEGURIDAD** La impresión de fondo de seguridad sirve de protección contra la falsificación y la manipulación de datos. Constituye la base de cualquier documento de identidad seguro y consiste en una variedad de elementos de seguridad individuales impresos, como guilloches, patrones de líneas finas o impresión del iris (arco iris). Los fondos de seguridad suelen crearse con un software especial de diseño de seguridad e imprimirse con equipos de impresión offset de seguridad de alta resolución.	Esta característica de seguridad puede verificarse sin utilizar dispositivos adicionales mediante el ojo humano. Además, utilizando un dispositivo de aumento, los distintos elementos pueden verse de forma independiente.
10	**MICROTEXTO FLUORESCENTE UV** Los elementos de microtexto fluorescentes UV consisten en letras o números impresos muy pequeños, apenas perceptibles a simple vista, pero que se hacen visibles cuando se iluminan con una fuente de luz UV y se observan con un dispositivo de aumento.	Este elemento de seguridad puede verificarse iluminando el documento con luz ultravioleta (365 nm).
11	**IMPRESIÓN BIFLUORESCENTE UV** En función de la longitud de onda UV bajo la que se examine el documento (313 nm frente a 365 nm), el color de la tinta UV bi-fluorescente (papel y policarbonato 365 nm / papel 254 nm / policarbonato 313 nm) cambia en consecuencia.	Esta característica de seguridad puede verificarse iluminando el documento con longitudes de onda cambiantes de luz ultravioleta (365 nm).
12	**TIPO DE LETRA NO ESTÁNDAR** Para dotar al documento de un símbolo de reconocimiento distintivo y de un aspecto único, se diseña un tipo de letra personalizado. El hecho de que este tipo de letra especial, no estándar, no esté disponible en el mercado comercial, dificulta aún más la imitación del documento. El uso de fuentes estándar revela una falsificación a primera vista.	Este dispositivo de seguridad puede verificarse con o sin el uso de dispositivos adicionales. Además, al utilizar sistemas de verificación asistidos por ordenador, el proceso de detección es mucho más rápido
13	**DISEÑO DÚPLEX** Los elementos de diseño de seguridad como el guilloche o el fractal se crean utilizando dos o más segmentos de color diferentes que se imprimen muy próximos entre sí (registro cercano). La técnica de impresión offset de seguridad utilizada tiene una resolución de 4.000 ppp y superior. Por esta misma razón, el documento no puede reproducirse con equipos de impresión comerciales sin cambiar visiblemente el aspecto visual y la integridad del diseño del documento.	Esta característica de seguridad puede verificarse sin utilizar dispositivos adicionales mediante el ojo humano. Además, utilizando un dispositivo de aumento se puede ver una ilusión.

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

EMDOC CONSORCIO

14	**TINTAS DE SEGURIDAD MIXTAS ÚNICAS** El diseño de fondo de un documento se imprime sin la selección comercial de colores CMYK ni las tintas planas estándar. En su lugar, todos los colores de seguridad utilizados se mezclan individualmente. La composición de estas tintas especiales es estrictamente confidencial y sólo la conocen la JCy el fabricante. La autenticidad de la tinta de seguridad puede verificarse mediante equipos de laboratorio.	Esta característica puede verificarse con un dispositivo de espectroscopia IR (cada composición de tinta puede almacenarse en una base de datos para su comparación).
15	**VENTANA TRANSPARENTE** La ventana transparente es un área definida del documento que es transparente. Está hecha de polímero y puede incluir opcionalmente otros elementos de seguridad o datos personalizados. Como la Ventana Transparente se produce durante un sofisticado proceso de fabricación y se incrusta en el cuerpo del documento, es muy difícil reproducirla sin dañar notablemente la estructura del documento.	Esta función de seguridad puede verificarse sin utilizar dispositivos adicionales mediante el ojo humano.
16	**IMAGEN DE TITULARES SECUNDARIOS (IMAGEN FANTASMA)** Una imagen fantasma o retrato del titular secundario es una reproducción semitransparente de la imagen personalizada del titular. Normalmente, esta imagen se sitúa en la misma cara que el retrato del titular principal o, lo que es aún más seguro, en el reverso del retrato del titular principal. La imagen semitransparente interactúa directamente con los elementos de fondo de seguridad del documento e impide así la manipulación o sustitución de la imagen facial.	Esta función de seguridad puede verificarse sin utilizar dispositivos adicionales mediante el ojo humano
17	**GUILLOCHE NEGATIVO** Los guilloches en negativo siguen las mismas reglas que los guilloches impresos normales, salvo que su forma no se crea imprimiendo líneas, sino rebajando deliberadamente el diseño de color circundante, creando así una imagen en negativo de las líneas de los guilloches, que aparecen como líneas blancas.	Esta función de seguridad puede verificarse sin utilizar dispositivos adicionales mediante el ojo humano
18	**GRABADO POR LÁSER** El grabado por láser es una de las técnicas de personalización de documentos más seguras. Los elementos de personalización visual en forma de imágenes en escala de grises, texto en negro y códigos de barras se graban con láser en una de las capas interiores del documento. En términos de seguridad de los documentos, el grabado por láser ofrece muchas ventajas: Por ejemplo, no sólo proporciona una resolución muy alta, que a su vez proporciona una calidad de imagen excelente y muestra los máximos detalles, sino que también garantiza una larga vida útil de los datos grabados personalizados. Las capas inseparablemente laminadas no pueden desmontarse sin dañar irreversiblemente toda la estructura del documento.	Esta función de seguridad puede verificarse sin utilizar dispositivos adicionales mediante el ojo humano

EMDOC CONSORCIO

19	**ESTRUCTURA LENTICULAR - IMAGEN LÁSER MÚLTIPLE (MLI)/IMAGEN LÁSER CAMBIANTE (CLI)** La tecnología MLI/ CLI es un elemento de seguridad ópticamente variable personalizado. Ya durante el proceso de producción, se graba en la superficie del documento un conjunto de lentes cilíndricas. Estas lentes contienen el MLI/ CLI, que se personaliza mediante grabado por láser y puede contener información específica del titular (por ejemplo, retrato del titular, fecha de nacimiento, número personal). Dado que el MLI/ CLI está grabado en varias capas del cuerpo del documento, es detectable forzosamente durante un análisis de laboratorio. Dado que la inclusión de un MLI/ CLI en un documento de seguridad requiere mucha experiencia y conocimientos técnicos (por ejemplo, en términos de ángulos de las lentes, ajustes del láser, etc.), es extremadamente difícil falsificarlo o imitarlo.	Esta función de seguridad puede verificarse sin ningún dispositivo adicional. Cambiando el ángulo de visión se puede ver información diferente dentro de la lente.
20	**ELEMENTO ÓPTICO DIFRACTIVO VARIABLE** Los hologramas son dispositivos de seguridad que contienen una amplia gama de elementos de seguridad adicionales, como microtexto, nanotexto, colores espectrales, guilloches, efectos tridimensionales o elementos holográficos especiales. Dependiendo de la iluminación o del ángulo de visión, el aspecto de los hologramas cambia en cuanto a color y diseño. El hecho de que el holograma esté protegido por numerosas capas inseparablemente laminadas dificulta enormemente la manipulación del documento sin dañar visiblemente su estructura.	Esta función de seguridad puede verificarse sin utilizar dispositivos adicionales cambiando la iluminación y/o la dirección de visión.
21	**MICROTEXTO EN EL INTERIOR DEL ELEMENTO ÓPTICO DIFRACTIVO VARIABLE** El microtexto difractivo o no difractivo, de hasta 175 micras de tamaño, es invisible a simple vista. Sólo puede verse con una lupa y una fuente de luz dirigida. Para crear microtexto son necesarios procesos especiales de producción holográfica. Por eso, este elemento de seguridad es muy difícil de copiar o imitar con equipos de impresión normales.	Esta característica de seguridad puede verificarse mediante inspección a través de una lupa e iluminación simultánea desde un ángulo específico.
22	**NANOTEXTO EN EL INTERIOR DE UN ELEMENTO ÓPTICO DIFRACTIVO VARIABLE** El nanotexto difractivo o no difractivo, con un tamaño de 40 a 175 micras, es invisible a simple vista. Sólo puede verse con un microscopio de alta potencia. Para crear nanotexto se requiere un proceso de producción holográfica especial. Por eso, este elemento de seguridad es casi imposible de copiar o imitar con equipos de impresión normales.	Esta característica de seguridad puede verificarse mediante inspección con microscopio (zoom 40x) e iluminación simultánea desde un ángulo específico.

CONSORCIO EMDOC EMDOC CONSORCIO 29 Santo Domingo, R.D.

EMDOC

23	**SUBSTRATO POLICARBONATO MATE UV** Esta característica de seguridad es una sofisticada extensión de la tinta fluorescente UV única. Se imprimen un mínimo de dos o más tintas fluorescentes monocolor en una de las capas interiores del documento. Al examinar el documento bajo una fuente de luz UV, cada tinta fluorescente UV brilla en un color diferente.	Este elemento de seguridad puede verificarse iluminando el documento con luz ultravioleta (365 nm).
24	**IMPRESIÓN ARCO IRIS FLUORESCENTE UV (IMPRESIÓN IRIS)** Esta característica es igual a la impresión del arco iris visible, pero ofrece una seguridad adicional, ya que se utilizan colores fluorescentes UV. Una separación de colores de los elementos de diseño UV se imprime la misma unidad de impresión en dos o más colores fluorescentes UV. Los diferentes colores fluorescentes UV se funden sin dejar espacios entre ellos. Este cambio continuo de color no puede copiarse sin un efecto de tramado claramente visible. La combinación de impresión visible y fluorescente UV en arco iris aumenta significativamente la protección contra falsificaciones de los documentos de identidad.	Este elemento de seguridad puede verificarse iluminando el documento con luz ultravioleta (365 nm)
25	**CONSTRUCCIÓN MULTICAPA** El documento de identificación final consta de varias láminas sintéticas, que juntas forman una construcción multicapa. Cada una de estas láminas contiene distintos componentes del documento, por ejemplo la antena, la parte impresa o la personalizada. Durante la producción, las distintas láminas se ensamblan, se intercalan y se laminan juntas a alta temperatura y presión, sin utilizar ningún tipo de pegamento. El resultado final es un monobloque de polímero que ya no puede separarse en las láminas individuales originales. Por lo tanto, esta construcción multicapa impide que los documentos puedan ser copiados o imitados: cualquier intento de separar las distintas capas del documento o de manipular los datos dañará las otras capas, de modo que quede en el documento una evidencia inmediatamente reconocible.	Este dispositivo de seguridad puede verificarse inspeccionando frontalmente el borde con una lupa.
26	**GRABADO LÁSER TÁCTIL** Los elementos perceptibles (táctiles), como texto, números o símbolos personalizados, pueden aplicarse a la superficie del documento mediante grabado por láser de última generación. Como este elemento de seguridad es irreversible, impide de forma fiable la alteración de información personalizada visualmente.	Este elemento de seguridad puede verificarse mediante inspección con ojo humano desde un ángulo agudo en relación con la superficie de la tarjeta. También puede detectarse hápticamente.
27	**TINTA ABSORBENTE DE INFRARROJOS Y TINTA TRANSPARENTE DE INFRARROJOS** Al visualizar el documento con una cámara de infrarrojos, la mayor parte del fondo se vuelve invisible. Sólo permanecen visibles los elementos grabados con láser o impresos con tintas absorbentes de IR. Esto proporciona protección contra la copia y la imitación, ya que las tintas IR no pueden escanearse ni copiarse	Este dispositivo de seguridad puede verificarse con una cámara de infrarrojos (iluminación de 870 nm).

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

EMDOC

28	**LEYENDA DE MICROTEXTO REPETITIVA (PANTALLA DE MICROTEXTO)** Una pantalla de microtexto está formada por elementos de microtexto. La diferente gradación tonal está formada por los distintos niveles de grosor de las microletras (grosor variable). Para aumentar aún más el nivel de seguridad del documento, esta técnica de tramado puede combinarse con errores ortográficos intencionados.	Estos elementos de seguridad pueden verificarse mediante inspección con lupa.
29	**PANTALLA FRACTAL** Esta técnica utiliza líneas individuales cuya dirección se controla mediante fórmulas matemáticas. Los distintos niveles de tonalidad se crean mediante diferentes tipos de grosor de línea. Para aumentar aún más la seguridad del documento, los errores intencionados también pueden incluirse en la Pantalla Fractal.	Esta característica de seguridad puede verificarse sin utilizar dispositivos adicionales mediante el ojo humano. Además, utilizando un dispositivo de aumento se puede ver una translación.
30	**NÚMERO DE SERIE PREPERSONALIZADO GRABADO CON LÁSER** Ya durante el proceso de fabricación, se aplica un número único al documento en blanco. Este número permite el seguimiento preciso de cada documento durante toda la cadena de producción y la gestión de todo el ciclo de vida. Gracias al número único, los documentos robados pueden identificarse sin problemas e invalidarse para evitar su uso indebido posterior.	Esta función de seguridad puede verificarse sin utilizar dispositivos adicionales mediante el ojo humano.
31	**SUPERFICIE TÁCTIL ESTRUCTURA EN RELIEVE** Esta estructura en relieve en la superficie del documento se aplica durante la producción del documento mediante el uso de placas especiales de laminación grabadas. El relieve consiste en líneas perceptibles u otros elementos de diseño, que aparecen en relieve positivo, negativo o mate en la superficie de los documentos. El preciso proceso de fabricación permite incluso integrar elementos de seguridad adicionales, como una imagen latente o un microtexto. Los intentos de separar las capas del documento o de reproducirlo en su totalidad serán reconocidos inmediatamente, ya que la superficie gofrada del documento quedará visiblemente dañada en cualquier caso.	Este dispositivo de seguridad puede verificarse sin utilizar dispositivos adicionales cambiando la iluminación y/o la dirección de visión. También se puede detectar háptica mente.
32	**TINTA LUMINISCENTE INFRARROJA (EFECTO ANTI-STOKES)** En este dispositivo de seguridad, la tinta luminiscente infrarroja se aplica a una de las capas internas del documento mediante una tecnología de impresión de seguridad de vanguardia. Durante el proceso de verificación, la energía activadora de la tinta luminiscente infrarroja es suministrada por un láser infrarrojo especial. El color absorbe fotones en la longitud de onda del infrarrojo cercano (980 nm) y emite varios colores en el espectro visible. Así, el rayo láser, que normalmente es invisible a simple vista, se	Este dispositivo de seguridad puede verificarse con una cámara de infrarrojos (iluminación de 980 nm).

	hace visible. Además de este método de verificación visible, la tinta luminiscente infrarroja también puede verificarse acústicamente.	
33	**PANTALLA DE ARTE** En comparación con las pantallas de microtexto, una Pantalla Artística se compone de caracteres únicos, signos y objetos como logotipos o símbolos que, en combinación con la modulación del grosor, forman los diferentes tonos. Para aumentar aún más la seguridad del documento, también se pueden incluir errores intencionados en la Pantalla de Arte.	Esta función de seguridad puede verificarse sin utilizar dispositivos adicionales mediante el ojo humano.
34	**MICROTEXTO DE TAMAÑO VARIABLE** Para dificultar aún más la imitación o la falsificación, el micro... El texto no se imprime en un tamaño uniforme, sino que varía en su interior.	Estos elementos de seguridad pueden verificarse mediante inspección con lupa
35	**PIGMENTOS FLUORESCENTES UV INCORPORADOS AL COLOR VISIBLE** Pigmentos invisibles, que sólo son fluorescentes bajo la luz ultravioleta, se añaden a la tinta offset visible. Elementos impresos con esta tinta mezclada aparecen tanto bajo la luz visible como bajo la UV ligera.	Este elemento de seguridad puede verificarse iluminando el documento con luz ultravioleta (365 nm).
36	**ELEMENTO OVD (TINTA IRIDISCENTE)** Las tintas iridiscentes contienen pigmentos semitransparentes que provocan interferencias con la luz incidente. Esto crea efectos brillantes, como perlas, que se hacen visibles o invisibles cuando cambia el ángulo de visión o la iluminación. Este efecto de brillo no puede copiarse, lo que contribuye aún más a la protección contra la falsificación del documento.	Esta característica de seguridad puede verificarse sin utilizar dispositivos adicionales mediante el ojo humano. Además, utilizando un dispositivo de aumento, los demás elementos pueden verse de forma independiente.

CONSORCIO EMDOC EMDOC CONSORCIO 32 Santo Domingo, R.D.

EMDOC CONSORCIO

1.5.5 Características electrónicas y sistema operativo

Los documentos de la tarjeta propuesta estarán equipados con un componente de chip que proporciona las siguientes funciones:

- Documento electrónico de viaje
- Firma electrónica
- Identificación del Ciudadano

Según los requisitos de la licitación, estas funcionalidades se ponen a disposición del titular de la tarjeta a través de una interfaz sin contacto. El componente de chip propuesto admite operaciones criptográficas respaldadas por hardware y almacena los datos correspondientes al menos diez años en la memoria no volátil.

Las funciones del documento no se modifican después de su expedición al ciudadano, por lo que no es aplicable una función posterior a la personalización.

1.5.5.1 Características del chip sin contacto

Este componente de chip propuesto para el documento de la nueva tarjeta electrónica proporciona un conjunto común de bloques funcionales e interfaces, compatible con aplicaciones de alto rendimiento, de interfaz sin contacto y sin contacto.

Equipado de este modo, este componente constituye una plataforma ideal para establecer en la tarjeta las aplicaciones deseadas para el Documento Electrónico de Viaje, la Firma Electrónica y la Identificación del Ciudadano. El chip propuesto reúne las siguientes características:

COMPONENTE CHIP	
Características	• CPU de 16/32 bits • Certificación CC EAL 6+ • Criptoprocesador hardware para operaciones criptográficas • Clave simétrica (Triple DES con clave de hasta 168 bits, AES de hasta 256 bits) • Clave pública (RSA con longitud de clave de hasta 4096 y ECC con longitud de clave de hasta 512 bits) • Hash SHA1 y SHA2 • Generador de números aleatorios según AIS31 • Protección ESD • Reloj interno asíncrono • Número de serie único • Cortafuegos de seguridad entre particiones de memoria • Memoria no volátil necesaria para la incorporación de las aplicaciones requeridas y los datos especificados en esta sección 1.2.4: 90 KB mínimo • Conservación de datos en memoria no volátil durante al menos 25 años • Al menos 2 millones de ciclos de lectura/escritura garantizados ISO/IEC 14443 Una interfaz RF de hasta 848 kbits/s, con capacidad para ofrecer modos de transmisión RF mejorados. • Opción UID aleatorio
Componente de chip	• Chip NXP P71, J3R180
Interfaz	• Interfaz sin contacto ISO/IEC 14443

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, RD 33

1.5.5.2 Características del sistema operativo

El sistema operativo propuesto está diseñado para circuitos integrados de seguridad de gama alta con interfaz sin contacto y potentes capacidades criptográficas mediante el uso de coprocesadores para el cifrado de claves públicas y secretas. El sistema operativo es realmente multiaplicación y cumple todas las normas abiertas pertinentes. También cuenta con la certificación Common Criteria.

El componente de chip y applet propuesto presenta las siguientes características técnicas:

Sistema operativo	
Características	El sistema operativo y el software de aplicación seleccionados proporcionan todas las funciones necesarias para un documento de identidad electrónico. Esto incluye una aplicación de viaje conforme con el Doc 9303 de la OACI, una identificación ciudadana y aplicaciones de firma electrónica. Con la posibilidad de bloquear la adición de nuevas aplicaciones una vez incorporadas las requeridas. La aplicación de la OACI dispone de las últimas funciones descritas por la OACI.
Apoyo de:	• Protocolo de transmisión según ISO/IEC 14443 A/B • Interfaz de comandos según ISO/IEC 7816-4 • UID aleatorio • Certificación Common Criteria EAL6+
Sistema operativo	• JCOP 4.0
Funciones:	• Documento electrónico de viaje conforme a la norma 9303 de la OACI • Firma electrónica • Identificación de los ciudadanos
Funcionalidades de los documentos electrónicos de viaje:	• SAC (Control de acceso suplementario) • EAC (Control de acceso ampliado) • AA (autenticación activa)

Funcionalidades de firma electrónica:	• Acceso protegido mediante PIN / PUK
	• Algoritmos de firma RSA y ECDSA
	• Soporte para claves RSA en formato CRT y en formato normal (exponente privado, exponente público y módulo).
	• Claves RSA compatibles con componentes q y de longitud variable p
	• Capacidad para almacenar, generar y utilizar claves RSA de al menos 4096 bits de longitud.
	• Compatibilidad con varias curvas ECDSA, incluidas las más comunes (NIST P-256, por ejemplo, Brainpool).
	• Operaciones de firma digital:
	  ○ Sesión o intercambio de claves simétricas entre dos entidades basado en RSA/ECDSA/ECDH
	  ○ Claves almacenadas en archivos/elementos separados
	  ○ Condiciones de acceso independientes para cada clave/elemento
	  ○ Estructura interna de archivos conforme a la norma ISO/IEC 7816-15 (PKCS#15)

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo

	○ Tendrá capacidad de memoria suficiente para almacenar hasta 4 certificados, con sus correspondientes claves, incluido el caso de claves RSA 4096. ○ Aseguramiento de los mensajes transmitidos entre la tarjeta y el terminal mediante canal seguro según CEN14890 o equivalente. ○ Confidencialidad de los datos transmitidos mediante triple DES / AES ○ Autenticación de la información intercambiada entre las dos partes; incorporación de suma de comprobación criptográfica de tipo MAC según ANSI X9.19 y DES. ○ La solución técnica ofrecida hace referencia a la RFC 3163 "ISO/IEC 9798-3 Authentication SASL Mechanism" que a su vez hace referencia a la ISO 9798-3. Para crear un mecanismo SASL de autenticación, se admiten los siguientes algoritmos de firma mencionados en la sección 4 de esta RFC: RSA-SHA1-ENC y ECDSA-SHA1 ○ Claves de sesión derivadas de la información generada por las partes implicadas en el establecimiento del canal seguro; las claves se calculan según ANSI X9.63.
Gestión de software y controladores	• Controladores de tarjeta (PKCS#11, CSP, módulo de tarjeta...) • Software de gestión que permite gestionar las operaciones más habituales con la tarjeta; por ejemplo, cambio de PIN, desbloqueo de PIN, borrado de certificados, etc. Asegura que el documento funciona en diferentes sistemas operativos (Windows, Linux, MacOS). Asegura que el documento funciona en diferentes navegadores. • Se proporcionan librerías o SDK que facilitan el desarrollo de aplicaciones para dispositivos móviles, con sistemas operativos Android e iOS. • El software suministrado se actualizará, adaptándolo a nuevos sistemas operativos, navegadores, corrección de errores, etc., durante la vida del proyecto.
Funciones de identificación de ciudadanos	• Los datos de afiliación del ciudadano se almacenarán de forma estructurada. • Se accederá a ellos por medios seguros. • De acuerdo con la Guía Técnica BSI TR-03110

CONSORCIO EMDOC EMDOC CONSORCIO 36 Santo Domingo, R.D.

EMDOC

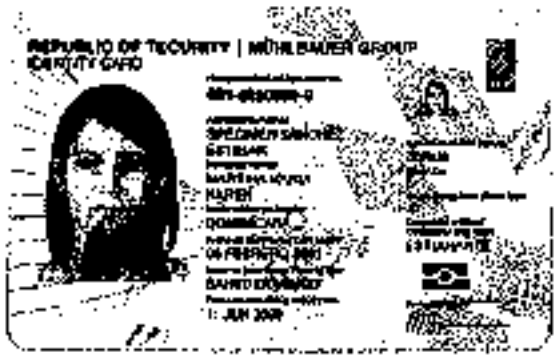
1.6 Tarjeta de muestra

1.6.1 Vista previa

1.6.1.1 Parte delantera



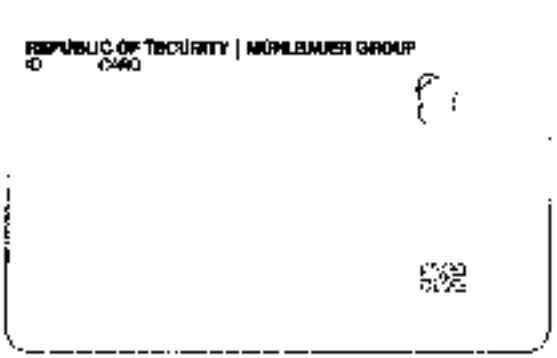
Vista previa del diseño de la tarjeta en blanco con luz normal



Vista previa del diseño de la tarjeta personalizada con luz normal



Vista previa del diseño de la tarjeta en blanco bajo luz ultravioleta



Vista previa del diseño de la tarjeta en blanco bajo luz IR

1.6.1.2 Parte trasera



Vista previa del diseño de la tarjeta en blanco con luz normal



Vista previa del diseño de la tarjeta personalizada con luz normal

37



Vista previa del diseño de la tarjeta en blanco bajo luz ultravioleta

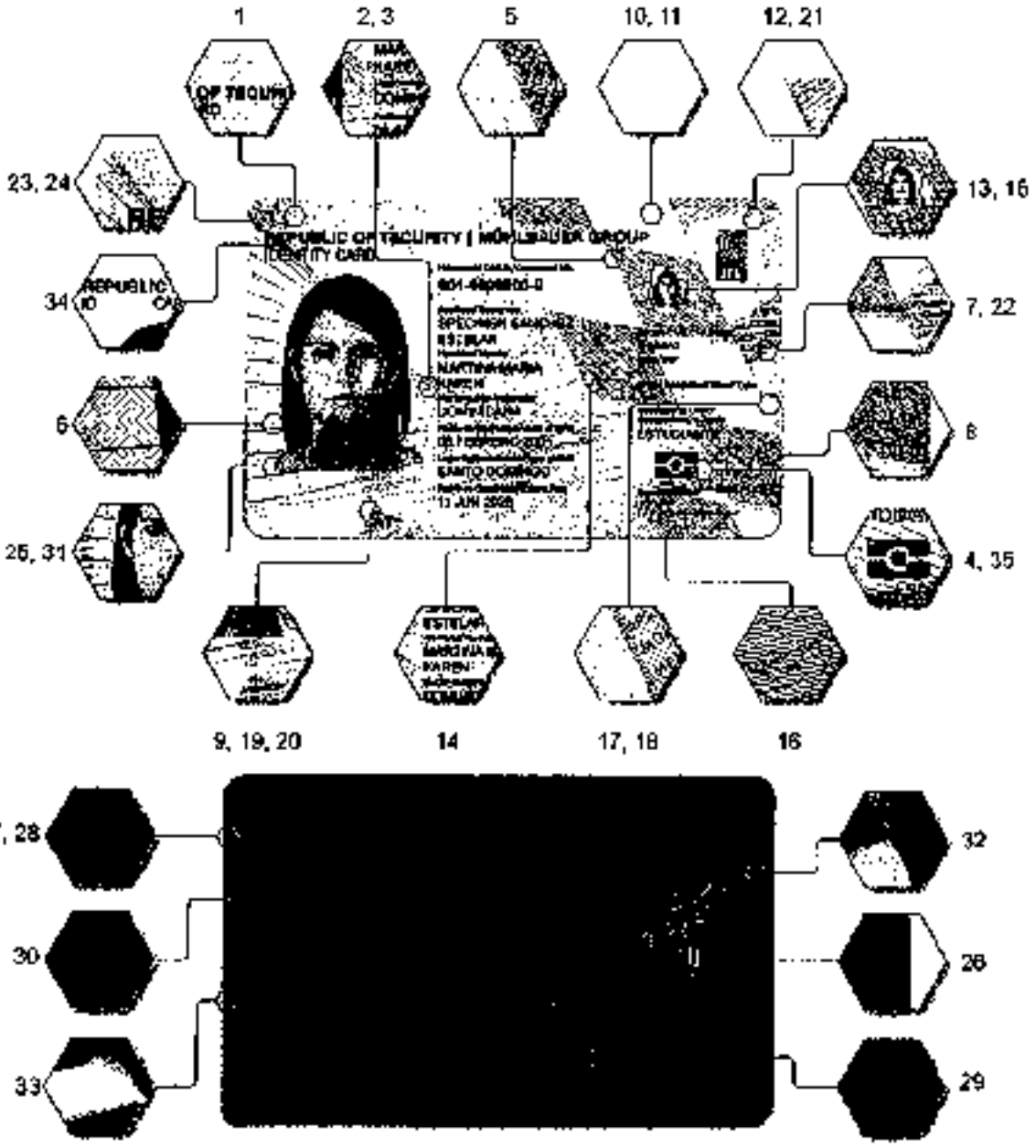


Vista previa del diseño de la tarjeta en blanco bajo luz IR

CONSORCIO EMDOC
EMDOC
CONSORCIO
37
Santo Domingo, R.D.

EMDOC CONSORCIO

1.6.2 Descripción general de las funciones de seguridad

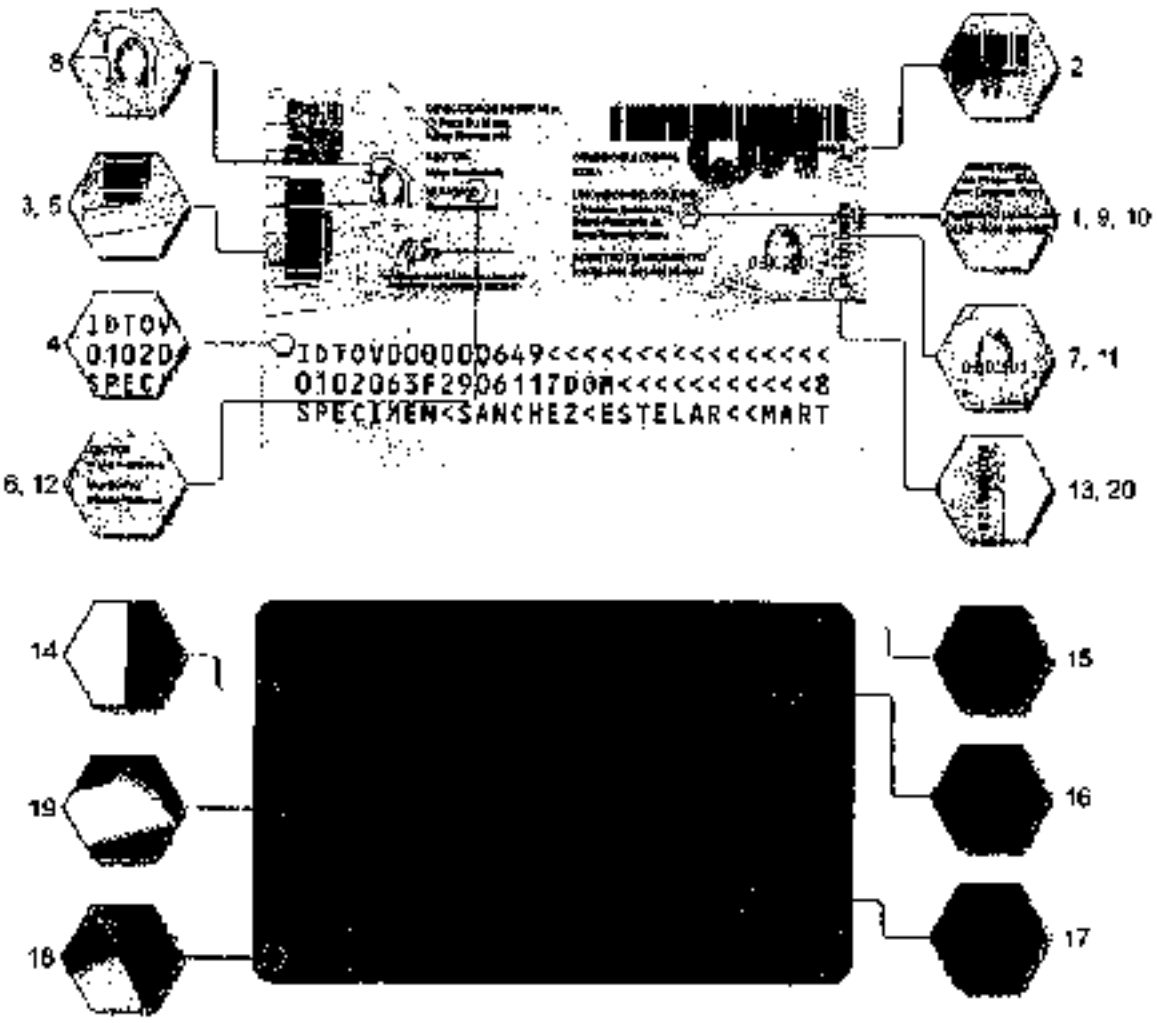


EMDOC

No.	Elemento de seguridad	No.	Elemento de seguridad
1	Impresión arco iris (Iris)	19	Microtexto en el interior de un elemento óptico difractivo variable
2	Guilloches	20	Nanotexto en el interior de un elemento óptico difractivo variable
3	Guilloches negativos	21	Leyenda de microtexto repetitiva (pantalla de microtexto)
4	Tinta Óptica Variable (OVI)	22	Pantalla de arte
5	Diseño 3D (numismático)	23	Microtexto de tamaño variable
6	Pantalla fractal	24	Tipo de letra no estándar para texto desplazado
7	Modulación de anchura de línea	25	Fondo de seguridad fusionado con el área de retrato (Protección de retrato)
8	Diseño dúplex	26	Material mate UV
9	Elemento óptico difractivo variable (parcialmente superpuesto Retrato del titular)	27	Microtexto fluorescente UV
10	Superficie táctil en relieve	28	Malla de microtexto de fondo fluorescente UV
11	Elementos táctiles (estructura en relieve de la superficie táctil) en altorrelieve	29	Impresión arco Iris fluorescente UV
12	Seguridad	30	Diseño fluorescente UV en la zona del retrato (protección del retrato)
13	Imagen del titular secundario (Imagen fantasma)	31	Fondo de seguridad visible e invisible en la zona del retrato
14	Grabado láser táctil	32	Tintas de seguridad mixtas exclusivas
15	Ventana transparente	33	Construcción multicapa (mínimo 5 capas)
16	Microtexto positivo	34	Tintas invisibles en IR
17	Microtexto negativo	35	Tinta luminiscente infrarroja (efecto antistokes)
18	Falta de ortografía deliberada dentro de un microtexto		

iQtek KURZ Muehlbauer GSI ULTRATECH VERIDOS

CONSORCIO EMDOC EMDOC CONSORCIO 39 Santo Domingo, R.D.



CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.
40

EMDOC

No.	Elemento de seguridad	No.	Elemento de seguridad
1	Impresión arco iris (iris)	11	Estructura lenticular (MLI) con imagen fantasma y fecha
2	Guilloches	12	Grabado por láser de datos personales
3	Guilloches negativos	13	Número de cuerpo de tarjeta único prepersonalizado grabado con láser (grabado táctil)
4	Modulación de anchura de línea	14	Material mate UV
5	Diseño dúplex	15	Impresión bi-fluorescente UV
6	Seguridad	16	Pigmentos fluorescentes UV incorporados al color visible
7	Imagen del titular secundario (imagen fantasma)	17	Impresión arco iris fluorescente UV
8	Ventana transparente	18	Tintas de seguridad mixtas exclusivas
9	Microtexto positivo	19	Construcción multicapa (mínimo 5 capas)
10	Deliberar error ortográfico dentro de microtexto	20	Grabado láser táctil

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D. A1

EMDOC CONSORCIO

1.7 Matriz de conformidad

Característica	Requisitos para la [illegible]	MUNDIPASS
Material		
Dimensiones según la normativa ISO/IEC 7816-2019 / ISO/IEC 7810:2019	✓	✓
Material: Policarbonato - mínimo 5 capas	✓	✓
Tintas de formulación específica para sistema de impresión offset - tintas de seguridad con pigmento sólido	✓	✓
Tintas ópticamente variables	✓	✓
Elemento holográfico	✓	✓
Todas las tintas deben cumplir la norma de durabilidad ISO 18745 y tener una solidez a la luz de 4 en la escala de lana azul.	✓	✓
Principales características de seguridad		
Diseño exclusivo de fondos de seguridad para imprimir en offset, contemplando guilloches, microtextos	✓	✓
Motivos impresos en al menos dos colores de tinta visible, que deben ser fluorescentes en el anverso al menos cuando se exponen a una luz ultravioleta.	✓	✓
Estampado en relieve mediante laminación en registro	✓	✓
Superficie lenticular para poder personalizar un CLI o MLI	✓	✓
Ventana transparente para definir su forma y posición en la tarjeta para imprimir las medidas de seguridad que contiene la solución como la fotografía y la fecha de caducidad de la tarjeta	✓	✓
Dispositivo de seguridad de las tarjetas - Nivel 1		
Impresión del Iris	✓	✓
Guilloches	✓	✓
Numismática/ Diseño 3D	✓	✓
Tinta ópticamente variable: aquella que contiene partículas finas en su superficie que proporcionan el efecto óptico con variabilidad cuando se cambia el ángulo de incidencia de la luz y observacional. Son visibles a IR.	✓	✓
Elemento difractivo ópticamente variable, situado en el interior de la tarjeta ocupando parcialmente la zona de la fotografía del Titular. Este elemento también puede incluir características de nivel 2 y 3	✓	✓
Dispositivo de seguridad de las tarjetas - Nivel 2		
Elementos táctiles en alto o bajo relieve o con acabado mate, integrados en la superficie de la tarjeta (en el anverso)	✓	✓
Personalización en relieve por láser del nombre y del número de la tarjeta	✓	✓
Microtextos - Positivos y negativos	✓	✓
Microtexto fluorescente	✓	✓
Malla de fondo UV en microtexto	✓	✓

CONSORCIO EMDOC EMDOC CONSORCIO 42 Santo Domingo, R.D.

EMDOC CONSORCIO

Errores deliberados en el documento	✓	✓
Tinta invisible que se vuelve fluorescente bajo la luz ultravioleta.	✓	✓
Impresión arco iris visible	✓	✓
Impresión arco iris invisible	✓	✓
Fondo de seguridad visible e invisible en la zona de la fotografía	✓	✓
Tipo de letra no estándar para elementos de texto desplazados	✓	✓
Dispositivo de seguridad de las tarjetas - Nivel 3		
Mínimo 5 capas	✓	✓
Tintas invisibles en infrarrojos	✓	✓
Nanotextos integrados en el elemento difractivo	✓	✓
Fondo de seguridad visible e invisible en la zona de la fotografía	✓	✓
Otros dispositivos de seguridad		
Ventana transparente con imagen fantasma y fecha de caducidad	✓	✓
Estructura lenticular: debe incluir una estructura lenticular para la personalización de una CLI	✓	✓
Elementos ópticos difractivos variables - parche difractivo transparente de diseño exclusivo, combinado con líneas de nanotexto y textos de formas moduladas en líneas sinusoidales. Las imágenes deben tener textos ocultos visibles en determinados ángulos de visión, que pueden cambiar en más de un ángulo	✓	✓
Protección del retrato del propietario - mediante un elemento de tipo ópticamente variable difractivo transparente, parcialmente coincidente con el retrato del propietario.	✓	✓
Numeración de tarjetas: cada tarjeta se identificará individualmente mediante un número de serie prepersonalizado grabado con láser.	✓	✓
Elementos de seguridad adicionales		
Diseño dúplex		✓
Elemento OVD (impresión iridiscente)	✓	✓
Guilloches negativos		✓
Pantalla de microtexto		✓
Impresión UV Bi-Fluorescent		✓
Pantalla de arte		✓
Tinta luminiscente infrarroja (efecto Anti-Stokes)		✓
Pantalla fractal		✓
Microtexto de tamaño variable		✓

CONSORCIO EMDOC EMDOC CONSORCIO 43 Santo Domingo, R.D.

EMDOC CONSORCIO

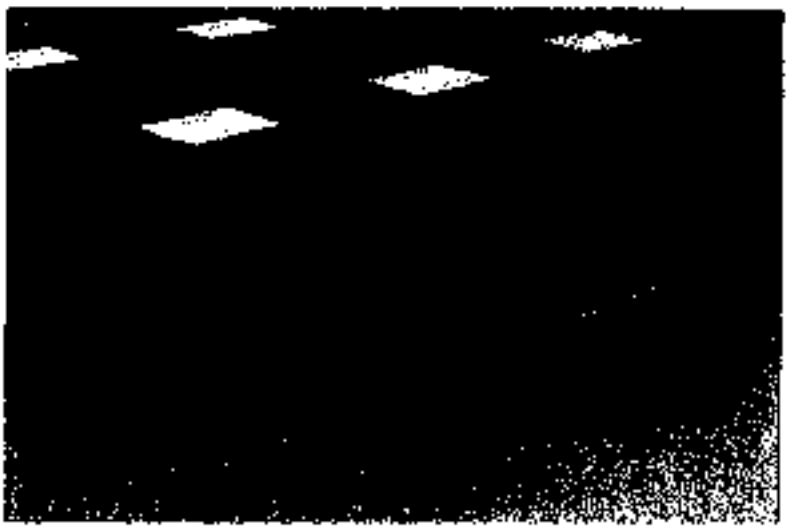
1.8 Embalaje y transporte

Cantidad de 1000 tarjetas en blanco prepersonalizadas (contactivas) embaladas en cajas de cartón blanco. La caja de cartón se retractila dos veces. La lámina de retractilado limitará el movimiento de las tarjetas durante el transporte y el almacenamiento en el almacén. La primera vez se retractila la parte inferior de la caja, donde se colocan las tarjetas con la etiqueta, y la segunda vez se retractila la parte superior de la caja, donde se coloca la misma etiqueta en la parte frontal. Las etiquetas colocadas en el interior y en la parte superior de la caja facilitan el seguimiento de las tarjetas. Estas cajas de tarjetas pueden reutilizarse en instalaciones de personalización de tarjetas para transportarlas

La información que contiene la etiqueta es:

- Fecha de envasado
- Nombre del producto
- Número de artículo
- Gama de números de serie
- Tipo de tarjeta
- Cantidad
- Número de casilla
- Código de barras

Las cajas de cartón se envasarán en papel de aluminio sellado al vacío para protegerlas de las cambiantes condiciones ambientales durante el transporte. Esta bolsa de aluminio se introduce en una caja de envío de dimensiones aproximadas 80x77x77cm. La caja de envío se fija en una paleta de madera y se sujeta con cinta de seguridad en cada lado con una etiqueta en la parte superior. Las cajas de envío están fabricadas con un tipo especial de cartón muy resistente para el transporte. Estas cajas son más respetuosas con el medio ambiente que los embalajes de madera.



Una vez que todo esté embalado y preparado, las cajas se cargarán en el camión utilizando el principio de los cuatro ojos con personal cualificado y formado para la manipulación de mercancías seguras. El envío saldrá de la zona de seguridad de producción con transporte de seguridad y siguiendo las recomendaciones de Intergraf. El transporte de seguridad se llevará a cabo hasta el destino final.

CONSORCIO EMDOC
EMDOC CONSORCIO
Santo Domingo, R.D.

EMDOC CONSORCIO

1.9 Entregables

Posición	Breve descripción de la configuración propuesta	Unidades	Comentario
1	Propuesta de diseño de seguridad	1	4 semanas después de la firma del contrato
2	Tarjetas genéricas de policarbonato con chip para pruebas	2,000	16 semanas después de la firma del contrato
3	Tarjetas de policarbonato y certificado de pruebas de un laboratorio certificado independiente	300,000	22 semanas tras la firma del contrato y la aprobación del diseño gráfico
4	Tarjetas de policarbonato	500,000	26 semanas tras la firma del contrato y la aprobación del diseño gráfico
5	Tarjetas de policarbonato	1,200,000	30 semanas tras la firma del contrato y la aprobación del diseño gráfico
6	Tarjetas de policarbonato	1,000,000	34 semanas tras la firma del contrato y la aprobación del diseño gráfico
7	Tarjetas de policarbonato	1,000,000	38 semanas tras la firma del contrato y la aprobación del diseño gráfico
8	Tarjetas de policarbonato	1,000,000	42 semanas tras la firma del contrato y la aprobación del diseño gráfico
9	Tarjetas de policarbonato	1,000,000	46 semanas tras la firma del contrato y la aprobación del diseño gráfico
10	Tarjetas de policarbonato	1,000,000	50 semanas tras la firma del contrato y la aprobación del diseño gráfico
11	Tarjetas de policarbonato	1,000,000	54 semanas tras la firma del contrato y la aprobación del diseño gráfico

CONSORCIO EMDOC EMDOC CONSORCIO 45 Santo Domingo, R.D.

EMDOC CONSORCIO

1.10 Derechos de propiedad

El Consorcio EMDOC entregará a la JCE a más tardar dos (2) semanas después de la aprobación del diseño final por la JCE

- Material gráfico final en formato digital (adobe, Corel Draw u otro formato editable)
- Material gráfico final para cada capa de diseño por separado
- Detalle de los elementos utilizados en la elaboración de los CI y CIE
- Guía física del arte por separación de colores
- Protocolos para la destrucción de bidones y placas utilizados en el proceso de producción de CI y CIE

1.11 Control de calidad

Si se encuentran tarjetas dañadas, deterioradas o defectuosas, Mühlbauer las sustituirá en un plazo no superior a treinta (30) días naturales desde la fecha de notificación.

Durante la recepción del suministro, el JCE probará aleatoriamente el producto para verificar las cantidades, el número de ejemplares y comprobar el estado de las tarjetas; reservándose el derecho de aceptar o rechazar la totalidad o parte del producto.
El Consorcio EMDOC proporcionará un manual impreso y otro en formato digital (Word y PDF) con instrucciones de uso y recomendaciones para manipular y salvaguardar las tarjetas.
El documento especificará, entre otras cosas, las condiciones ambientales y de infraestructura recomendadas del lugar donde se almacenarán.

Todo ello se dirigirá al Director de Cedulación de la JCE, Santo Domingo, República Dominicana.

CONSORCIO EMDOC EMDOC CONSORCIO 46 Santo Domingo, R.D.

EMDOC CONSORCIO

2 Términos de referencia

2.1 Punto I: Especificaciones técnicas de las tarjetas

Posición	Requisito	Comentario
I.1	**Características generales** El diseño de todas las características y elementos de seguridad debe utilizar soluciones tecnológicas especializadas en el sector de la identidad y cumplir la normativa Doc 9303 de la OACI Las tarjetas son un elemento clave y deben ser fabricadas por un miembro del consorcio. Se solicitan tarjetas de policarbonato para los nuevos CI y CIE, con chip sin contacto con funcionalidad de Documento Electrónico de Viaje, Firma Electrónica e Identificación Ciudadana. A continuación se detallan las características técnicas de las tarjetas:	Conforme, consulte el capítulo 1Documentos de la tarjeta
I.2	**Tipos de tarjetas** El adjudicatario deberá suministrar los siguientes tipos de tarjetas: ▲ Identidad y Tarjeta Electoral • Tarjeta para el carné de identidad. Las tarjetas deben tener las mismas características físicas estipuladas para las dos tarjetas, variando únicamente en cuanto al color de la tarjeta (fondos preimpresos) y la personalización del reverso.	Conforme, consulte el capítulo 1.2Tipos de tarjetas
I.3	**Formato del documento** Las dimensiones y sus tolerancias se especificarán mediante el formato **ID-1** especificado en ISO/IEC 7816:2019 / ISO/EC 7810:2019. **Característica** / **Valor mínimo** / **Valor máximo** Espesor / 0,68 mm / 0,84 mm Largo / 85,47 mm / 85,72 mm Anchura / 53,92 mm / 54,03 mm Será una tarjeta sin contacto conforme a las normas ISO/IEC 14443 vigentes.	Conforme, consulte el capítulo 1.1Características generales

CONSORCIO EMDOC EMDOC CONSORCIO 47 Santo Domingo, R.D.

I.4	**Materiales** • Tarjeta de polímero termoplástico (policarbonato) de alta resistencia, formada por varias capas (5 como mínimo) fusionadas mediante laminación resistente a la rotura en caliente. • Tintas de formulación específica para el sistema de impresión offset. • Tintas de seguridad con pigmento sólido. • Tintas ópticamente variables. • Elemento holográfico/ OVD. Todas las tintas deberán cumplir la norma de durabilidad (ISO 18745) y tener una solidez a la luz de 4 en la escala de lana azul.	Conforme, consulte el capítulo 1.1Características generales
I.5	**Principales elementos de seguridad** Los diseños de seguridad del documento serán entregados por el adjudicatario al JCE en archivos vectoriales en formato electrónico. El JCE será el propietario de todos los derechos sobre estos diseños. En resumen, explicado con más detalle a continuación, las tarjetas tendrán: • Diseño exclusivo de los fondos de seguridad a imprimir en offset, contemplando guilloches, microtextos combinados con motivos o imágenes alegóricas a la República Dominicana, formados por líneas finas continuas con modulación de su grosor u otros patrones de alta seguridad • Motivos impresos en al menos dos colores de tinta visible, que deben ser fluorescentes en el anverso al menos cuando se exponen a una fuente de luz ultravioleta. • Estampado de superficies en relieve mediante laminación en registro. • Estructura lenticular para poder personalizar un CLI o MLI. • Ventana transparente para definir su forma y posición en la tarjeta para imprimir las medidas de seguridad contenidas en la solución, como la fotografía de la tarjeta y la fecha de caducidad.	Conforme, consulte el capítulo 1.4Principales medidas de seguridad
I.6	**En cuanto al sistema de personalización**	Conforme, consulte el capítulo 1.4Principales medidas de seguridad

	Personalización de datos variables mediante grabado láser, siendo para fotografía láser con impresión en escala de grises.	
I.7	**Otras características** Inclusión de un chip sin contacto con funcionalidad de documento de viaje electrónico de la OACI (véase el documento lógico para las características electrónicas y del sistema operativo en este documento).	
I.8	**Características detalladas**	
I.8.1	**Elementos de seguridad de la tarjeta**	
I.8.1.1	**Nivel 1 - Elementos de seguridad que se detectan y verifican mediante una simple inspección visual:** • Impresión en iris: líneas que cambian gradualmente de color durante su recorrido sin interrupción del trazo. • Guilloches: movimientos lineales ornamentales que se componen de múltiples curvas entrelazadas, elaboradas simultáneamente, formando complejos diseños creados mediante programas informáticos de seguridad. • Numismática: conjunto de líneas que sufren una deformación en su recorrido y cuya combinación da sensación de relieve o volumen. • Tinta ópticamente variable: la que contiene en su estructura partículas finas que dan el efecto óptico de variabilidad cuando se cambia el ángulo de incidencia de la luz y la observación. Son visibles en la radiación IR. • Elemento difractivo ópticamente variable, situado en el interior de la tarjeta, que ocupa parcialmente la zona de la fotografía del titular de la tarjeta. Como se explica más adelante, este elemento también puede incluir medidas de nivel 2 y, en algunos casos, de nivel 3. • Elementos táctiles en alto o bajo relieve o con acabado mate, integrados en la superficie de la tarjeta. Personalización en relieve con personalización láser del nombre y el número de tarjeta.	Conforme, consulte el capítulo 1.5.1Funciones de seguridad de nivel 1, 2 y 3
I.8.1.2	**Nivel 2 - Elementos de seguridad que requieren el uso de instrumentos sencillos, como lupas de aumento y bombillas, para su detección:**	Conforme, consulte el capítulo 1.5.1Funciones de seguridad de nivel 1, 2 y 3

	• Microtextos. Impresión en positivo y negativo. Microtexto de fluorescencia. • Malla de fondo microtexturada UV. • Errores deliberados en el documento. • Tinta invisible que se vuelve fluorescente bajo la luz ultravioleta. Impresión arco iris visible (impresión arco iris offset). Impresión arco iris invisible (impresión arco iris por fluorescencia UV) • Fondos de seguridad visibles e invisibles en la zona fotográfica para detectar posibles manipulaciones o sustituciones de la fotografía. • Tipo de letra no estándar para elementos de texto impresos.	
L8.1.3	**Nivel 3 - Elementos de seguridad forenses que requieren detección en laboratorio:** • Tarjeta multicapa de 5 capas como mínimo. • Tintas invisibles en el Infrarrojo (para permitir la lectura mecánica del documento. Exigencia de la OACI). • Nanotexturas integradas en el elemento difractivo. • Fondos de seguridad visibles e invisibles en la zona fotográfica para detectar posibles manipulaciones o sustituciones de la fotografía.	Conforme, consulte el capítulo 1.5.1Funciones de seguridad de nivel 1, 2 y 3
L8.1.4	**Otros dispositivos de seguridad** • **Elemento óptico difractivo variable:** Parche difractivo transparente de diseño exclusivo para el JCE, combinado con líneas de Nanotextos y textos de formas modulades en líneas sinusoidales. Las imágenes tendrán textos ocultos visibles en determinados ángulos de observación que podrán ser modificables en más de un ángulo. • **Elementos táctiles:** Se integrarán en la estructura de la tarjeta, en el anverso de la misma, durante el proceso de fabricación. El diseño de estos elementos deberá ser aceptado por la CEB. • **Ventana transparente:** Incluirá una ventana transparente.	Conforme, consulte el capítulo 1.5.1Funciones de seguridad de nivel 1, 2 y 3 Y 1.5.2Otros dispositivos de seguridad

CONSORCIO EMDOC EMDOC CONSORCIO 50 Santo Domingo, R.D.

	• **Estructura lenticular:** Incluirá una estructura lenticular para la personalización de una CLI. • **Protección del retrato del titular:** Mediante un elemento difractivo transparente ópticamente variable, parcialmente coincidente con el retrato del titular. • **Numeración de las tarjetas:** Cada tarjeta se identificará individualmente mediante un número de serie de tarjeta grabado con láser prepersonalizado	
I.8.1.5	**Resistencia de la tarjeta conforme a la OACI** • **Durabilidad:** La durabilidad del soporte estará garantizada por un período de 10 años. • **Deformación:** De tal naturaleza que la deformación causada por el uso normal puede enderezarse con el equipo de lectura sin afectar al uso de la tarjeta o a su funcionamiento. • **Toxicidad:** No debería presentar ningún riesgo tóxico en condiciones normales de uso. • **Resistencia a los productos químicos:** Deberá ser resistente a los efectos químicos inherentes a su manipulación y uso normal, excepto cuando se le haya cotado de sensibilidad química por razones de seguridad. • **Estabilidad térmica:** Permanecerá legible mecánicamente a temperaturas comprendidas entre -10 °C y +50 °C. La tarjeta no perderá su funcionalidad si se expone a temperaturas que oscilen entre -35 °C y +80 °C. • **Humedad:** La tarjeta deberá ser legible por la mécuina a una humedad relativa ambiente del 5 % al 95 % y a una temperatura máxima de bulbo húmedo de 25 °C en . La tarjeta no perderá su fiabilidad si se almacene o se expone a una humedad relativa ambiente del 0 % al 100 % (sin condensación).	Conforme, consulte el capítulo 1.5.3Resistencia de la tarjeta según la OAC
I.9	**Características electrónicas y sistema operativo** Las funcionalidades electrónicas estarán operativas una vez que se realice una activación mediante una comparación 1:1 cuando el ciudadano recoja su tarjeta.	Conforme

	Así se garantiza que la pérdida de una tarjeta no sirva de nada al malhechor, ya que la tarjeta no se activará y será inútil. Además de anular el plástico que tiene su numeración desde que sale de la fábrica donde se fabrica, el chip añade seguridad adicional, ya que su funcionalidad no esté activa hasta que la recoge el titular de la tarjeta. La nueva tarjeta estará equipada con tres funcionalidades electrónicas: • Documento electrónico de viaje. • Firma electrónica. • Identificación ciudadana. Para adaptarse a un número considerable de posibilidades de lectura eficaz y ágil mediante tecnologías sin contacto como Bluetooth, se ha decidido que la interfaz de comunicaciones sea únicamente por radiofrecuencia. Esto permitirá su uso en dispositivos móviles a través de la interfaz NFC, además de su uso en ordenadores. No está previsto que el documento pueda cambiar o ampliar su funcionalidad una vez entregado al ciudadano, con la excepción de los certificados de firma digital que pueden tener una fecha de caducidad diferente a la del documento físico, en cuyo caso la administración de todo el ciclo de vida del mismo (generación, actualización y revocación) debe estar prevista en los documentos electrónicos, para el resto de funcionalidades y como queda claro en el siguiente apartado que describe las características del chip (hardware) del Sistema Operativo que corre sobre él (software asociado), imprescindible para utilizar algunas de las funcionalidades descritas.	
1.9.1	**Características del chip sin contacto** • CPU de 16/32 bits. • Certificación CC EAL5+ o superior (o equivalente) • Criptoprocesador hardware para operaciones criptográficas. • Clave simétrica (Triple DES con clave de hasta 168 bits, AES de hasta 256 bits). • Clave pública (RSA con longitud de clave de hasta 4096 y ECC con longitud de clave de hasta 512 bits). • Hash SHA1 y SHA2. • Generador de números aleatorios según AIS31 Protección ESD. • Reloj interno asincrono Número de serie único. • Cortafuegos de seguridad entre particiones de memoria. • Memoria no volátil necesaria para la incorporación de las aplicaciones requeridas y los datos especificados en este	Conforme, consulte el capítulo 1.5.5.1Características del chip sin contacto

	apartado 1.2.4. • Conservación de datos en memoria no volátil de al menos 10 años. • Al menos 500.000 ciclos de lectura/escritura garantizados Interfaz RF ISO/IEC 14443 A/B de hasta 848 kbit/s y puede ofrecer modos de transmisión RF mejorados.	
I.9.2	**Características del sistema operativo** • Protocolo de transmisión según ISO/IEC 14443 A/B Interfaz de mando según ISO/IEC 7816-4 y PCSC. • UID / PUPI aleatorio. • Certificación Common Criteria EAL4+ o superior (o equivalente). • En caso de que el Sistema Operativo esté basado en JavaCard, deberá bloquearse la posibilidad de añadir nuevas aplicaciones una vez incorporadas las necesarias. Incluirá las siguientes funcionalidades: • Documento electrónico de viaje conforme a la norma 9303 de la OACI. • Firma electrónica. • Identificación ciudadana. Funcionalidad de documentos electrónicos de viaje: Debe ser capaz de resistir: • SAC (Control de Acceso Suplementario). • EAC (control de acceso ampliado). • AA (autenticación activa) **Funcionalidad de firma electrónica:** • Acceso protegido mediante PIN / PUK. • Algoritmos de firma RSA y ECDSA. • Soporte para claves RSA en formato CRT y en formato normal (exponente privado, exponente público y módulo) • Claves RSA con soporte para componentes p y q de longitud variable. • Capacidad para almacenar, generar y utilizar claves RSA de al menos 4096 bits de longitud. • Compatibilidad con varias curvas ECDSA, incluidas las más comunes (NIST P-256, Brainpool, etc.). • Operaciones de firma digital.	Conforme, consulte el capítulo 1.5.5.2Características del sistema operativo

CONSORCIO EMDOC CONSORCIO Santo Domingo, RD

- Intercambio de claves simétricas o de sesión entre dos entidades basado en RSA/ECDS/ECDH.
- Claves almacenadas en archivos/elementos separados.
- Condiciones de acceso independientes para cada clave/elemento.
- Estructura interna del fichero según ISO/IEC 7816-15 (PKCS#15).
- Tendrá capacidad de memoria suficiente para almacenar hasta 4 certificados, con sus correspondientes claves, incluido el caso de claves RSA 4096.
- Securización de los mensajes transmitidos entre la tarjeta y el terminal mediante un canal seguro según CEN14890 o equivalente.
- Confidencialidad de los datos transmitidos mediante triple DES / AES.
- Autenticación de la información intercambiada entre las dos partes; incorporación de suma de comprobación criptográfica de tipo MAC según ANSI X9.19 y DES.
- Protocolo de establecimiento de clave de sesión basado en el esquema propuesto en ISO/IEC 9798-3 Authentication SASL Mechanism.
- Claves de sesión derivadas de la información generada por las partes implicadas en el establecimiento del canal seguro; las claves se calculan según ANSI X9.63.
- Software de gestión y controladores:
    - Controladores de tarjeta (PKCS#11, CSP, módulo de tarjeta, etc.).
    - Software de gestión para gestionar las operaciones más habituales con la tarjeta, por ejemplo, cambio de PIN, desbloqueo de PIN, borrado de certificados, etc. Debe garantizar el funcionamiento del documento en diferentes sistemas operativos (Windows, Linux, MacOS). Debe garantizar el funcionamiento del documento en diferentes navegadores.
    - Se deben proporcionar librerías o SDK que faciliten el desarrollo de aplicaciones para dispositivos móviles, con sistemas operativos Android e IOS.
    - El software suministrado debe actualizarse, adaptándolo a nuevos sistemas operativos, navegadores, corrección de errores, etc., durante la vida del proyecto.

Funcionalidad de identificación de los ciudadanos:

- Los datos de afiliación del ciudadano se almacenarán de forma estructurada.
- Se accederá a ellos por medios seguros.

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

EMDOC CONSORCIO

	• Preferiblemente de conformidad con la Guía Técnica TR-03110 de BSI o similar.	
	Muestras: El licitante deberá, al momento de presentar las ofertas, suministrar diez (10) tarjetas genéricas de policarbonato, con las mismas especificaciones técnicas solicitadas para esta licitación y con el detalle y explicación de las medidas de seguridad que el licitante está ofreciendo, explicando en un documento, cuales son los requisitos técnicos cumplidos y las medidas de seguridad ofrecidas, a excepción del diseño. Este es un requisito obligatorio (de obligado cumplimiento) que no puede ser subsanado.	Conforme, consulte el capítulo 1.6Tarjeta de muestra1.5Características detalladas / Características de seguridad de la tarjeta y 1Documentos de la tarjeta

CONSORCIO EMDOC EMDOC CONSORCIO 55 Santo Domingo, RD

36

ÍTEM II. MÁQUINAS DE IMPRESIÓN

PARA LA CONTRATACIÓN DE LA EMPRESA QUE SE ENCARGARÁ DE SUPLIR LOS EQUIPOS, MATERIALES Y SERVICIOS PARA LA IMPRESIÓN DE LA CÉDULA DE IDENTIDAD Y ELECTORAL (CIE) Y CÉDULA DE IDENTIDAD (CI)

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

Contenido

1 **MÁQUINAS DE IMPRESIÓN** 3
1.1 Máquina de Impresión 3
1.1.1 Módulo de alimentación de tarjetas (entrada) 6
1.1.2 Codificación de chips 6
1.1.3 Sistema de control de tarjetas para ajuste del láser 7
1.1.4 Respuesta a Seleccionar (ATS) por sistema de lectura del Módulo de Garantía do Calidad 7
1.1.5 Sistema láser 8
1.1.6 Sistema de control de tarjetas 9
1.1.7 Módulo de Salida 10
1.2 Sistema de control de máquina de impresión Mühlbauer MCES 10
1.2.1 Importación de datos 11
1.2.2 Base de datos MCES 11
1.2.3 Herramienta de registro 11
1.3 Funciones informáticas 12
1.3.1 Personalización Interfaz del sistema de la máquina de impresión 12
1.3.2 Máquina de impresión PC Interno 16
1.3.3 Integración en la red 16
1.4 Interfaz de usuario 17
1.4.1 Acceso para operadores 17
1.4.2 Edición del diseño de la tarjeta por personal autorizado 18
1.5 Personalización 20
1.6 Personalización según el formato y el diseño solicitados 20
1.6.1 Formato (Lay out) de las tarjetas ICN 20
1.6.2 Formato (Lay out) de las tarjetas CI 20
1.7 Sistema de desarrollo de software 22
1.7.1 Sistema de desarrollo de software MCES (SDK, APIS) 22

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

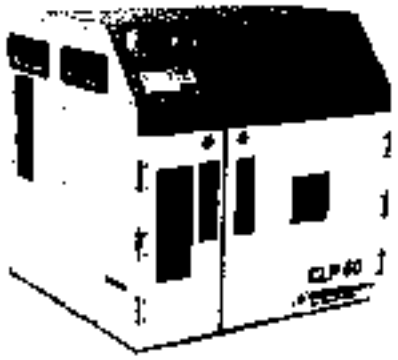
58

1. Máquinas de Impresión

1.1. Máquina de Impresión

Para la personalización de las tarjetas de identificación (Tarjeta de Identidad y Electoral (CIE) y Tarjeta de Identidad (CI), el Consorcio EMDOC propone el Sistema de Personalización de Tarjetas Inteligentes CLP 60 de Mühlbauer.

Se trata de un sistema de escritorio que ofrece excelentes resultados de personalización en cuanto a rendimiento y calidad de impresión de tarjetas en un espacio mínimo. El sistema se basa en la tecnología de grabado por láser que puede alinearse perfectamente con las tarjetas de policarbonato.



Impresora de tarjetas inteligentes de escritorio que permite una personalización de máximacalidad y seguridad, ocupando el mínimo espacio. Impresión de tarjetas con intervención humana mínima.

Además, la máquina de impresión ofrece un alto nivel de automatización, ya que las tarjetas sin personalizar se introducen en un alimentador de entrada desde que los documentos se individualizan automáticamente y se envían a los procesos de flujo de trabajo para la codificación de chips y el grabado por láser dentro del sistema de la máquina de impresión.

Al final de la cadena de procesos incorpora un módulo completo de control de calidad que controla los datos personalizados visualmente y los datos personalizados electrónicamente antes de que un documento o una tarjeta personalizada pase a la bandejade salida.

Utilizando este sistema el Consorcio EMDOC brindará a la JCE el cumplimiento de las recomendaciones de la Organización de Aviación Civil Internacional (OACI), según las cuales debe existir la menor intervención humana posible durante el proceso de personalización de documentos de alta seguridad.

Caracteristicas Generales de la Máquina de Impresión

- Concepto de máquina de impresión de escritorio.
- Diseño modular de la máquina de impresión para las estaciones de personalización.
- Módulos para grabado láser en escala de grises, codificación de chips, sistema de cámara para reconocimiento de tarjetas, sistema de cámara y lector para garantía de calidad de la personalización.

CONSORCIO EMDOC Santo Domingo, R.D.

- El sistema se ha desarrollado desde el punto de vista del diseño para satisfacer tanto las exigencias industriales como las de un entorno de oficina. Permite el funcionamiento de la máquina de impresión en 3 turnos (24 horas).
- Diseñado para ayudar a los operadores a manejar los documentos de forma sencilla y cómoda.
- Separación de tarjetas sin fricción para evitar arañazos.
- Protección de acceso al alimentador de entrada de tarjetas.

Rendimiento.

- Velocidad de Producción de 50 tarjetas por hora, incluido el grabado por láser, la codificación y el control de calidad.

Conformidad

- El sistema está diseñado para procesar tarjetas de formato ID-1 con un grosor de 0,76 mm ± 0,08 mm según la norma ISO/IEC 7810. Todas las especificaciones técnicas indicadas se basan en estas características técnicas.
- Compatibilidad con ISO 14443 Tipo A y B para el procedimiento de codificación de chip sin contacto.
- Apoyo a las recomendaciones del ICAO Doc. 9303, mediante la reducción al mínimo de la intervención humana y la personalización visual, basándoseen las especificaciones de la zona de inspección visual y la zona de lectura mecánica (MRZ).
- Codificación de Capacitación personal (demográfica y biométrica) en el chip (por ejemplo, grupos de datos ICAO 9303, claves y certificados).
- Integración de la Infraestructura Nacional de Clave Pública PKI (MRTD) para generar datos y presentar los grupos de datos ICAO 9303, para la firma digital por el Firmante de Documentos (DS).

Los sistemas de la máquina de impresión están diseñados para cumplir la normativa internacional de seguridad, como:

- Desarrollo, diseño y fabricación de los equipos de conformidad con las directivas de la CE:
  - 2006/42/CE para las máquina de impresión
  - 2014/30/UE para la compatibilidad electromagnética
- Conformidad CE
- Los sistemas láser incluyen cubierta diseñadas para cumplir la clase láser 1 según la norma ANSI Z136.1

Características técnicas

- Alimentación mediante conexión monofásica de 110/220 V para el funcionamiento
- Alimentacion mediante conexión monofásica de 230 V para el funcionamiento
- Fuente de alimentación ininterrumpida para cubrir las PC´s integradas producción durante al menos 2 minutos.

CONSORCIO EMDOC Santo Domingo, R.D.

Dimensiones

- Peso de la máquina de impresión aprox. 75 kg en total
- Tamaño de la máquina de impresión aprox. 0,6 m x 0,6 m (L x A) o 0,36 m² (Sujeto a la configuración final de la máquina de impresión).

Interfaz Gráfica de Usuario

- Pantalla táctil LED en color de 4,5" integrada para visualizar el estado de la máquina de impresión y los trabajos.
- Monitor adicional independiente para un manejo intuitivo de la máquina de impresión (Consulte también las descripciones del capitulo1.4Interfaz de usuario
-

Eficacia de la producción

La eficiencia de producción de los sistemas de máquina de impresiones propuestos será superior al 90% siempre:

- los lotes de producción adecuados se transfieren a las máquina de impresións para que, cuando se miden en consecuencia, no se produzcan interrupciones debidas a la selección y activación de los trabajos.
- el sistema lo maneja personal cualificado y está en buenas condiciones técnicas.
- los módulos de entrada se rellenan con el material necesario.
- suministro ininterrumpido de insumos y sin interrupción de la producción.
- disponibilidad permanente y estable de los medios técnicos y las condiciones del entorno de producción.

Calidad de las Impresoras

La unidad láser, integrada en el sistema de la máquina de impresión, tiene una vida útil de 20,000 horas de funcionamiento. Durante este periodo, la calidad del sistema láser puede cambiar. Sin embargo, este cambio puede reajustarse dentro de este periodo para que el resultado de grabado producido permanezca estable.

Para ello, se lleva a cabo la correspondiente validación láser como parte del mantenimiento preventivo. Para ello se personaliza una tarjeta de prueba, que se mide con un densitómetro de color y se evalúa con respecto a una tarjeta de referencia. Si el resultado de la medición está fuera de la tolerancia acordada, se reajusta el láser.

Si, a pesar del uso normal, el sistema láser o cualquier otro componente es tan defectuoso que ya no se puede lograr la calidad de personalización requerida, el sistema láser y el componente respectivo se sustituyen para que se restablezca la funcionalidad.

Gracias a su diseño, el sistema es fácil de mantener. En caso necesario, los componentes pueden desmontarse y sustituirse por otros nuevos. En este contexto, el fabricante garantiza la disponibilidad de piezas de repuesto durante toda la duración del contrato.

CONSORCIO EMDOC Santo Domingo, R.D.

Garantía
La garantía de la impresora de tarjetas es de 2 años

Configuración

- Alimentador de entrada de las tarjetas
- Identificación de la tarjeta (lectura del número de tarjeta)
- Módulo de codificación de chip, compatible con la codificación de chip basada en contacto o sin contacto según ISO 14443 Tipo A y B
- Sistema láser Sistema de visión inclusivo:
  - Alineación de la posición del láser
  - Sistema láser 20W (LES 20FP) con unidad giratoria CLI
- Garantía de calidad (comprobación de caracteres latinos / números / foto)
- Bandeja de Salida de tarjetas
- Plataforma de software de personalización (MCES II) con base de datos SQL Integrada

Documentación
El manual de instrucciones contiene detalles sobre:

- Seguridad
- Operación
- Servicio

y se facilitará en lengua española.

1.1.1. Módulo de alimentación de tarjetas (entrada)

El módulo alimentación de entrada de tarjetas está equipado con un eje de entrada de tarjetas que proporciona una capacidad de carga de 200 tarjetas.

Características del Módulo de Entrada

- Eje de entrada de tarjetas bloqueable para limitar el acceso a las tarjetas vírgenes
- Individualización de tarjetas sin fricción para evitar arañazos

1.1.2. Codificación de Chips

El módulo de codificación de chip se utiliza para la personalización eléctrica del módulo CI de una tarjeta inteligente.
El procedimiento utilizado para comunicarse con el chip y transferir datos se implementa mediante una DLL de codificación del chip, que se adapta / desarrolla individualmente en alineación con las características de la tarjeta proporcionadas por el fabricante de la tarjeta, incluye:

- Tipo de chip utilizado
- Tipo de sistema operativo

CONSORCIO EMDOC CONSORCIO Santo Domingo, RD

- Software de tarjeta en el chip
- Funcionalidades en el chip para el acceso seguro a los recursos de almacenamiento en la tarjeta en las funciones de autenticación y cifrado del chip, en relación con el proveedor de claves de seguridad, de modo que el resultado de la personalización cumpla las normas exigidas, como el Doc. 9303 de la OACI u otras normas aplicables.

1.1.3. Sistema de Control de Tarjetas para Ajuste del Láser

Este módulo de inspección de visión se utiliza para reconocer la posición de la tarjeta con el fin de crear un archivo de corrección, que contieneCapacitación de posicionamiento de rotación para el sistema láser para toda la Capacitación de personalización incluyendo la característica de CLI, independiente de otros elementos de datos para ser grabado con láser.

Características Generales

- Procesos de aprendizaje y comprobación del diseño controlados por software.
- Herramientas informáticas de análisis para aumentar el rendimiento de la producción.

Puestos de trabajo

- Unidad de fijación de tarjetas para resultados de inspección repetibles.
- Dispositivo de inspección mediante sistema de cámara de alta resolución.
- Dispositivo de iluminación LED para ajustes de iluminación individuales controlados por software. El sistema permite utilizar iluminación LED múltiple con diferentes longitudes de onda (ajuste de los canales R, G, B e IR).

1.1.4. Respuesta a Seleccionar (ATS) por sistema de lectura del Módulo de Garantía de Calidad

Todas las máquina de impresión disponen de un control de funcionamiento del chip (por ejemplo, prueba ATS) que tiene lugar antes de que la tarjeta entre en los módulos de personalización visual. Una tarjeta con un chip detectado como no funcional no se personaliza y se envía al compartimento de rechazo.

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

EMDOC

1.1.5. Sistema láser

Característica	Descripción
Sistema de grabado en escala de grises de alto rendimiento **Mühlbauer LES 20 FP**	
Tipo	Láser de fibra óptica
Medio	Iterbio
Longitud de onda	~ 1.064 nm
Potencia de salida	20 W
Ancho de pulso	Ajustable
Resolución	Rango de ajuste: 300 – 1.200 ppp Ajuste de funcionamiento: 600 dpi posible
Refrigeración	Aire - Aire
Materiales adecuados	Policarbonato Material

Marcaje láser
 
 
	Capacidad para grabar en superficies de capa frontal y posterior de materiales de tarjetas 100% policarbonato, incluyendo características como:
	
	• Imágenes, firmas, logotipos en escala de grises
	• Datos de texto (fuentes TTF)
	• Gráficos vectoriales y rasterizados (imágenes, firmas);
	• Códigos de barras 1D y 2D comunes (incl. PDF417 y QR-Codes)
	• Admite funciones de seguridad como:
	  ○ ventana transparente;
	  ○ imagen fantasma;
	  ○ elementos táctiles;
	  ○ Imagen láser intercambiable (CLI);
	  ○ Microtexto en línea recta y ondulada, formas.
	• En tamaños y posiciones variables definidas con el cliente;
	• Línea legible por máquina de impresión en la parte inferior del reverso de la tarjeta (MRZ).
	
	Elementos especiales de seguridad
	• Capaz de ofrecer imágenes de microtexto nítidas y definidas, como una línea de microtexto personalizada.

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

EMDOC
CONSORCIO

Es posible utilizar fuentes de tipo no estándar para el proceso de grabado láser. Estas fuentes deben ser Tue Type Fonts, para ser instaladas en SO WINDOWS.

El sistema láser permite personalizar las funciones de seguridad de acuerdo a:

- Nivel 1
- Nivel 2
- Nivel 3

1.1.6. Sistema de Control de Tarjetas

Una vez realizada la personalización óptica, se verificará la integridad y calidad de los datos personalizados. Las tarjetas se comprobarán por el anverso y el reverso.

Por ello, la máquina de impresión está equipada con una función de aseguramiento de la calidad automatizada, que incluye una comprobación total de los datos personalizados.

La verificación de los datos se realiza continuamente durante el funcionamiento del sistema y se aplica a cada tarjeta.
Las tarjetas que no cumplen los requisitos de calidad se clasifican y se transfieren a un compartimento de rechazo. Tal evento y las tarjetas afectadas serán debidamente etiquetadas en el sistema de control de la máquina de impresión, de donde tales datos pueden ser proporcionados alSistema de Gestión de Producción.



Para un procedimiento adecuado de aseguramiento de la calidad, el sistema está equipado con hardware y software de inspección específicos. Estos permiten:

- Evaluación del rendimiento de los chips
- Personalización correcta del chip, datos correctos del chip
- Control de la Capacitación grabada
    - Captura de imagen, firma, texto y otras características mediante un sistema de cámara que incluye unidades de iluminación
    - Verificación de datos de texto impreso o datos numéricos
    - Medición de la posición X-Y de los elementos impresos y comprobación de las tolerancias configuradas
    - Coincidencia de imagen y firma, mediante valor umbral ajustable (datos gráficos)
    - Correspondencia de códigos de barras (disponible para códigos de barras 1D / 2D, PDF-417, QR-Codes)
    - Control MRZ
    - Orientación y referencia de las tarjetas
- Mecanismo de prevención de doble separación de tarjetas

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

Características generales del sistema de visión

- Proceso de aprendizaje y comprobación del diseño controlado por software
- Herramientas informáticas de análisis para aumentar el rendimiento de la producción
- Unidad de arreglo de tarjetas para un resultado de inspección repetible
- Dispositivo de inspección mediante sistema de cámara de alta resolución
- Dispositivo de iluminación LED o ajustes individuales de iluminación controlados por software (diferente longitud de onda)

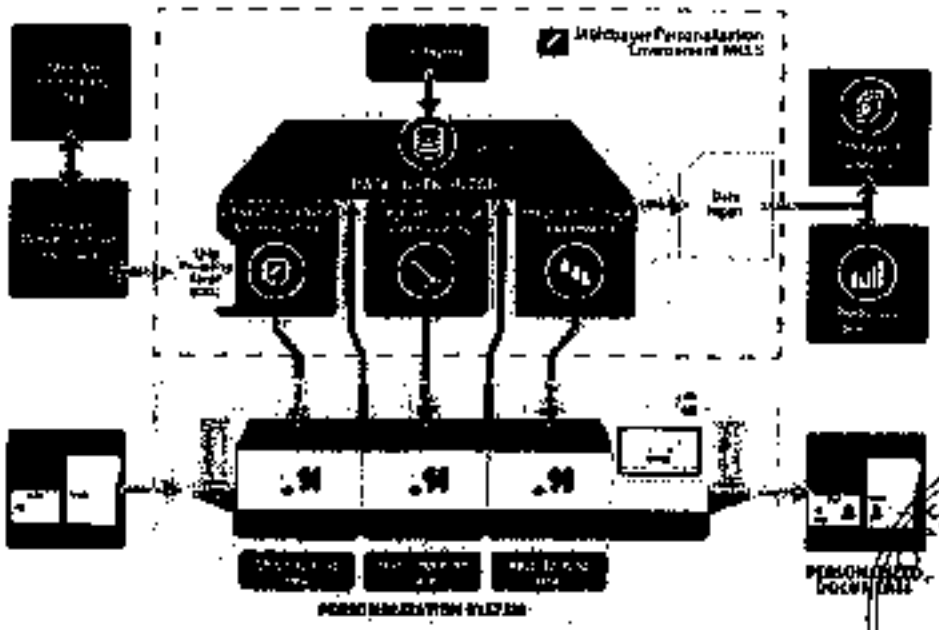
En función del resultado de la inspección, la tarjeta se dirige al compartimento de rechazos (tarjeta defectuosa) o a la bandeja de salida de tarjetas impresas correctamente.

1.1.7. Módulo de Salida

El módulo de salida de tarjetas está equipado con un compartimento de rechazo y una bandejade salida de tarjetas impresas correctamente. La bandeja de salida de tarjetas buenas proporciona una capacidad de carga de 200 tarjetas.

1.2. Sistema de control de máquina de impresión Mühlbauer MCES

El MCES de Mühlbauer se ha diseñado para satisfacer perfectamente las necesidades de la gestión de todos los datos de documentos y trabajos para una máquina de impresión de personalización de cualquier tipo, desde equipos de alto volumen hasta equipos de personalización de escritorio como la que se incluye en esta propuesta



MCES II proporciona interfaces para:

- Importación de datos
- Informes de personalización
- Supervisión

Además se admiten las siguientes funciones:

- Plugins de intercambio de datos
- Plugins de correspondencia de datos
- Plugins de codificación de chips con la interfaz de seguridad correspondiente

La interfaz de seguridad puede utilizarse para la conexión HSM, la conexión con firmantes de documentos, etc. Por norma, las interfaces se basan en XML. Pero también pueden implementarse formatos de datos personalizados. La gestión interna de datos utiliza una base de datos SQL.

1.2.1. Importación de datos

La importación de datos puede considerarse como el canal de datos hacia el sistema de la máquina de impresión. A través de este canal se envían a la máquina de impresión todos los datos relevantes para la personalización de las tarjetas de cédulas. La configuración de esta propuesta cumple una conexión TCP/IP utilizando el formato de datos XML. El módulo de adquisición se puede configurar libremente para conectarse a cualquier fuente de datos.

1.2.2. Base de datos MCES

Uno de los componentes más importantes es una base de datos interna de la máquina de impresión en el Sistema Maestro que enlaza las diferentes estaciones de trabajo de la máquina de impresión. La comunicación completa en el sistema de la máquina de impresión se organiza utilizando la base de datos ‚MCES, como intercambio central de Capacitación. De este modo, el tratamiento de los datos se garantiza de forma segura y coherente.

1.2.3. Herramienta de registro

El seguimiento de las acciones realizadas en un sistema de máquina de impresión moderno es una necesidad funcional. Por este motivo, se implementa una herramienta de registro en el sistema maestro para realizar un seguimiento de cada paso del proceso que se lleva a cabo en y desde el sistema. Se crea un archivo de registro a partir del cual se pueden generar informes estadísticos con Capadilación como:

- Registro de operadores
- Documentos tramitados con éxito en un plazo definido
- Documentos rechazados en un plazo definido
- Tiempo medio de personalización
- Cantidad de documentos personalizados por operador
- Resultado de la producción en una hora
- Tipos de rechazo detectados

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

- Etc.

Los datos de los informes sobre los documentos personalizados con éxito o los documentos no válidos detectados pueden generarse y enviarse a un sistema externo mediante el formato XML.

1.3. Funciones Informáticas

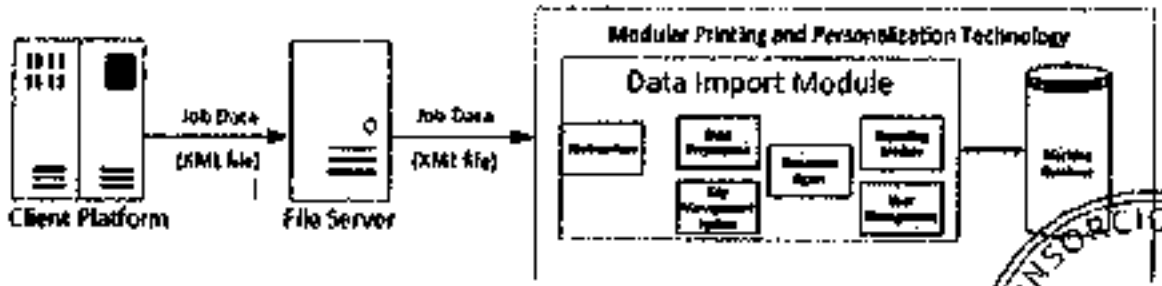
1.3.1. Personalización Interfaz del sistema de la máquina de impresión

Todos los sistemas de las máquinas de impresiónes propuestos están equipados con el software de gestión de personalizaciónMCES. Esta plataforma cuenta con una importación de datos que se utiliza para transferir datos de personalización a la máquina de impresión.

La Importación de datos puede considerarse como el canal de datos hacia el sistema de la máquina de impresión. A través de este canal, todos los datos relevantes para la personalización se envían a la máquina de Impresión para personalizar los documentos.

El formato del fichero de personalización es XML. El archivo XML se recibe de la plataforma de datos de la JCEen el servidor de archivos. Contiene todos los datos preparados para la personalización.

El software de Gestión de Personalización de Máquina de Impresión utiliza su Módulo de Importación de Datos para cargar automáticamente los archivos de trabajo de personalización desde el servidor de archivos a la máquina de impresión. Una vez cargado el archivo de trabajo de personalización en la máquina de impresión, ésta estará lista para la personalización.



EMDOC
CONSORCIO

Se supone que el suministro de datos se realiza mediante un sistema establecido y proporcionado por el cliente. Esto significa que este sistema transfiere datos de personalización (Datos Personales, Datos Biométricos, Datos de Control, Datos de Chip).

Cada archivo XML contiene un trabajo de personalización completo con los datos de personalización de un documento. La plataforma envía los archivos XML a carpetas específicas de la máquina de impresión situadas en el servidor de archivos. El software de gestión de personalización importa los archivos XML desde la carpeta asignada en el servidor de archivos.

El diseño de la impresión con imágenes, fotos, logotipos, textos, características especiales de seguridad como CLI o códigos de barras en la tarjeta, se puede configurar mediante la colocación de las características de marcado y especificar temas como el tipo de fuente y tamaños de fuente en un editor de diseño y guardar esta configuración como producto de personalización para un tipo dedicado de documento:

- Tarjetas CIE
- Tarjetas CI

En este contexto, siempre que sea factible, se tiene en cuenta:

- que el marcado armonice con la disposición especificada de la tarjeta y, en su caso, con una leyenda preimpresa en la tarjeta
- que se cumplan las normas especificadas por el cliente, como la OACI 9303, otras a través de la Interfaz del Sistema de Personalización de Máquina de Impresión, la Importación de Datos del Software de Gestión de Personalización MCES se utiliza para cargar los datos de personalización en formato de datos XML.

Preparación de datos, incoherencia, firma de documentos, función de gestión de claves

La interfaz del equipo de impresión modular recibe los datos generados por la JCE en archivos XML para personalizarlos. El equipo de impresión modular incorpora un módulo de preparación de datos para preparar los datos para realizar la personalización de las credenciales de forma totalmente automática. El módulo integrado de preparación de datos prepara los datos de acuerdo con las funciones conformes con la OACI para preparar automáticamente los datos según el tipo de documento que se vaya a personalizar.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

El sistema de gestión de claves integrado proporciona una herramienta de gestión fácil de usar para gestionar claves (simétricas y asimétricas) y el conjunto de llaves que vienen con el chip antes de la personalización. Con esto, el sistema de gestión de claves proporciona los servicios criptográficos para la preparación de datos para permitir, por ejemplo, la autenticación activa y la función de autenticación de chip de la aplicación de chip. Además, el sistema proporciona servicios de cifrado para el cifrado/descifrado de datos. El KMA gobierna las claves (por ejemplo, los Datos de habilitación del chip) y las claves/certificados que controlan la carga de la aplicación de la tarjeta (Acceso a la carga de la aplicación), la eliminación (Acceso a la eliminación de la aplicación) y la ejecución en el chip. Este sistema integrado de gestión de claves funciona automáticamente en la tecnología de personalización modular.

El módulo visual de firma de documentos integrado firma digitalmente todos los datos almacenados en el documento de identidad electrónico. También utiliza un HSM como entorno protegido para la generación y el almacenamiento del par de claves DS, y realiza funciones criptográficas con claves largas de acuerdo con la norma ICAO 9303. El firmante de documentos integrado genera solicitudes de certificados del documento signer (DS) y exporta la solicitud al CSCA. Una vez firmada la solicitud por la CSCA, el nuevo certificado DS se importará en el módulo DS integrado. El módulo DS integrado recibe la solicitud de firma de los datos del documento de identidad y envía una respuesta con los datos firmados a un módulo de preparación de datos/personalización (DP). Estas solicitudes y respuestas se intercambian entre el módulo DS y el módulo de preparación de datos, en el que el módulo de preparación de datos solicita la firma de los datos al firmante del documento. Los datos firmados se almacenan en el DG.SOD en el sistema de archivos del chip y todo el proceso funciona automáticamente en la tecnología del sistema modular de personalización.

Apoyo a la presentación de informes

Se asume que el sistema central de la JCE contiene un componente que permite transformar las actividades registradas por las máquinas de impresión para la personalización en un formato adecuado, para su posterior procesamiento.

La máquina de impresión de personalización proporciona una herramienta de registro, que rastrea las acciones realizadas en cada paso del proceso que se lleva a cabo en y desde el sistema. Los datos pueden almacenarse hasta 4 semanas. Puede tratarse de Capacitación como

- Registro de operadores
- Tarjeta de cédula tramitado con éxito en un plazo definido
- Tarjetas de cédulas rechazadas en un plazo determinado

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

- Tiempo medio de personalización
- Cantidad de tarjetas de cédulas personalizados por operador
- Resultado de la producción en una hora
- Tipos de rechazo detectados

Los datos pueden recogerse como un archivo de registro en formato de datos XML y transferirse a un sistema superior para su posterior procesamiento (por ejemplo, procesamiento gráfico, consolidación con otras máquina de impresións de personalización, etc.).

El sistema de la máquina de impresión apoya el proceso de creación de informes mediante la creación de un archivo de registro, que se transmite como Capacitación de gestión a un componente de creación de informes.

Almacenamiento temporal de datos

Para la personalización de la tarjeta, los datos necesarios del ciudadano se almacenarán localmente en la máquina de impresión CLP 60, sólo mientras dure el proceso de producción.

Tras la personalización de cada trabajo de producción, la máquina de impresión de personalización generará automáticamente un informe que contendrá el resultado de la personalización de todas estas tarjetas. La plataforma de personalización MCES II del CLP 60 eliminará los datos de registro temporales necesarios y almacenados.

CONSORCIO EMDOC Santo Domingo, R.D.

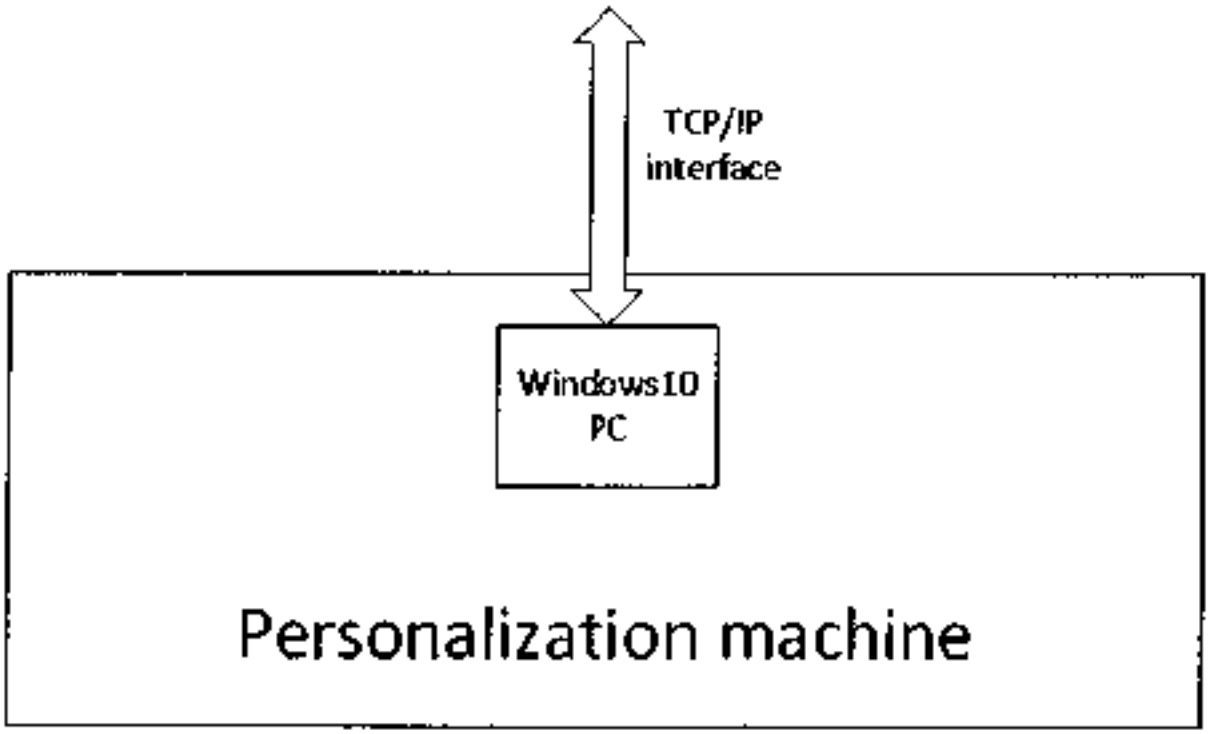
1.3.2. Máquina de impresión PC interno

El sistema está equipado con un PC interno (PC principal). El PC interno utiliza el sistema operativo Windows 10.



1.3.3. Integración en la red

Los sistemas propuestos están equipados con un PC principal que proporciona una interfaz de red (TCP/IP). La dirección IP correspondiente puede definirse y ajustarse a su debido tiempo.



CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

EMDOC CONSORCIO

1.4. Interfaz de usuario

Las máquinas de impresión de personalización propuestas están equipadas con un sistema de gestión de usuarios que regula el acceso al sistema.

Creación de grupos de usuarios como para:

- Nivel de administradores y supervisores
- Nivel de operador
- Nivel de servicio



Ajuste de:

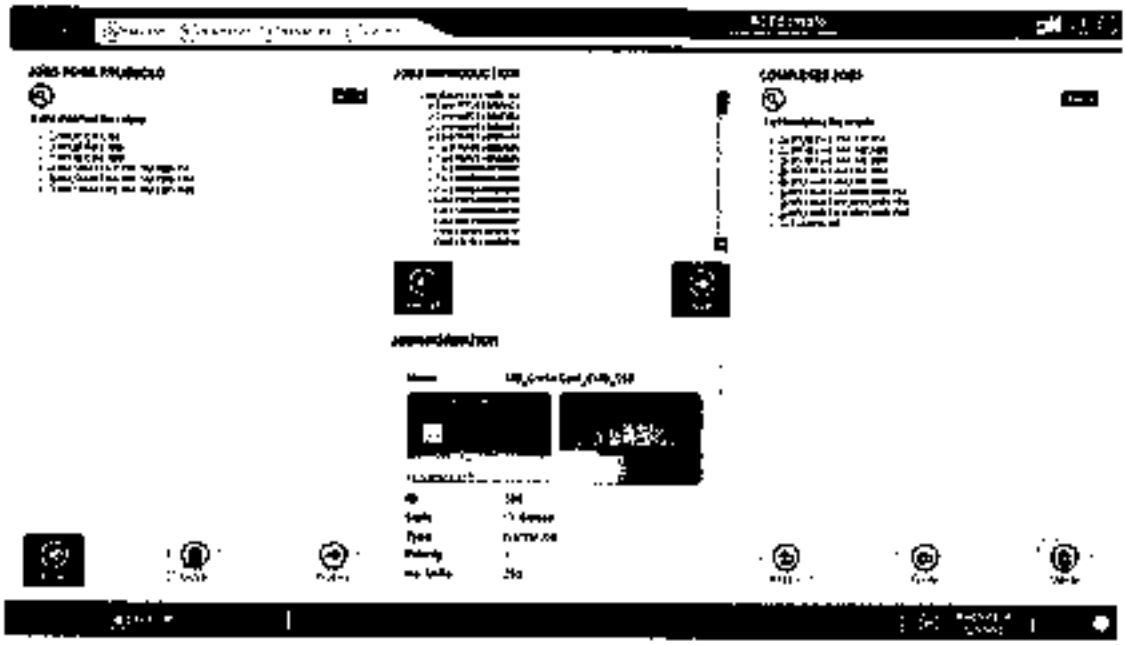
- Complejidad de las contraseñas, listas negras de contraseñas
- Cierre de sesión automático (en caso de que el usuario no interactúe o se solucione después de un tiempo determinado)

Posibilidad de asignar usuarios y grupos de usuarios a usuarios o grupos de usuarios del dominio

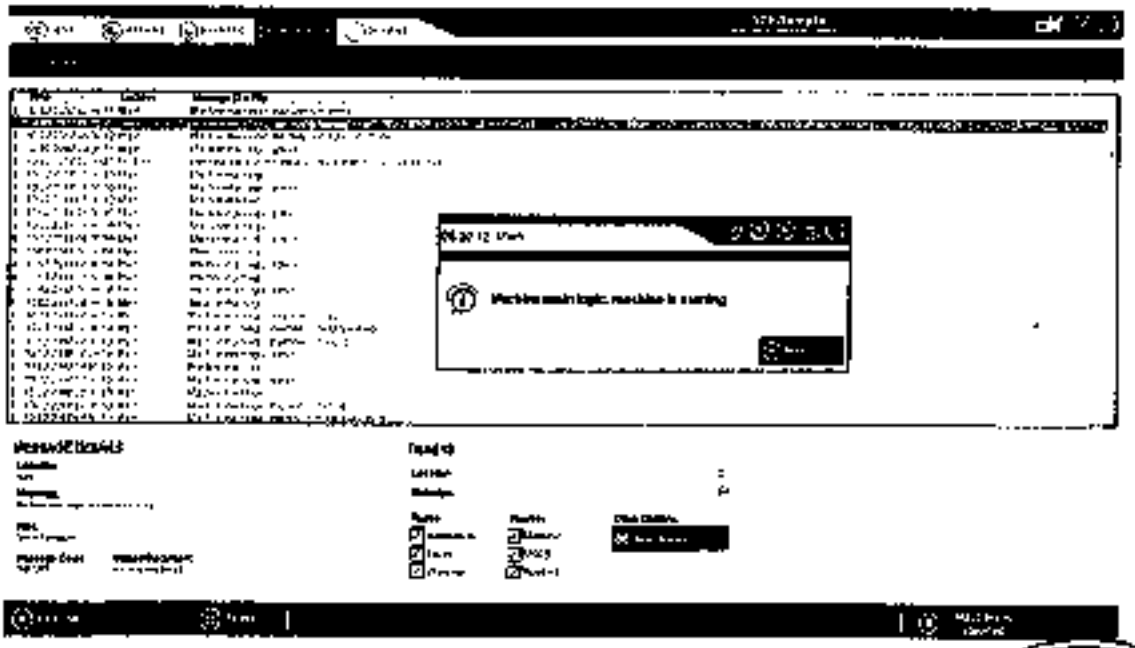
1.4.1 Acceso para operadores

Para el operario, sólo se hacen accesibles las funciones liberadas por el sistema interno de gestión de usuarios de la máquina de impresión. Pueden ser las siguientes:

- **Página Trabajos** - para ilustrar los trabajos de producción asignados a la máquina de impresión de personalización y para seleccionar y activar un trabajo de personalización.



- **Panel de mensajes:** enumera todas las actividades y proporciona mensajes de error e Capacitación de ayuda.



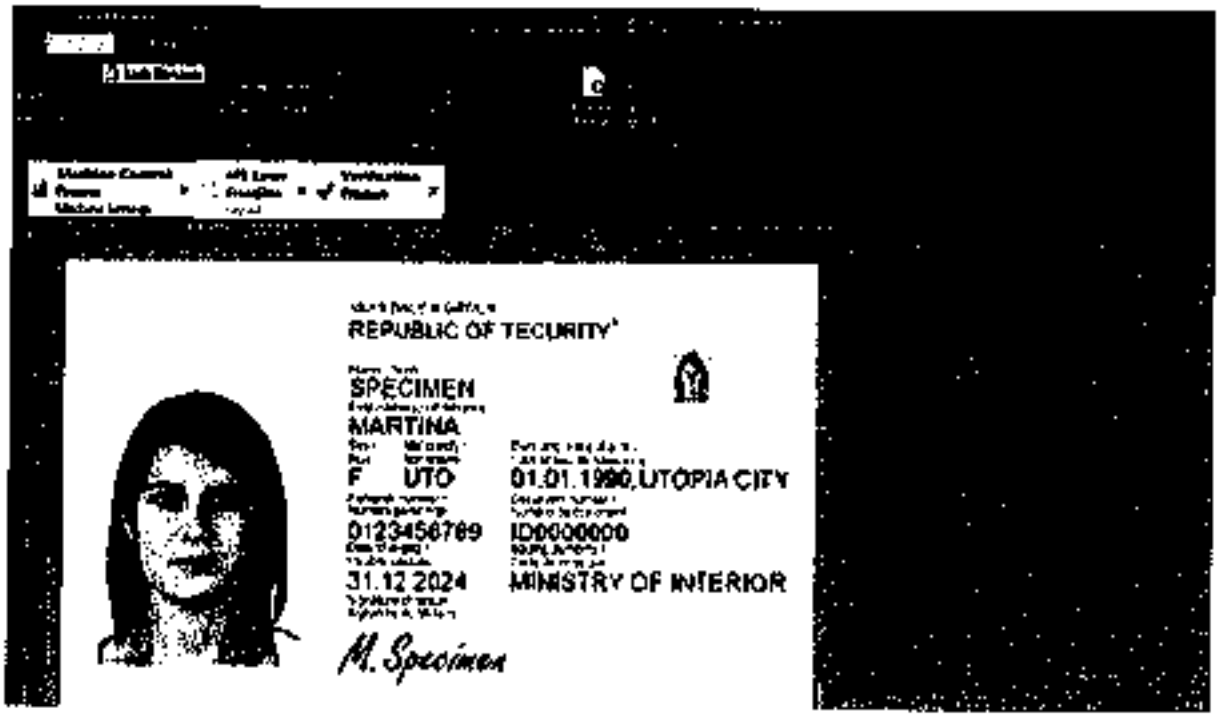
1.4.2. Edición del diseño de la tarjeta por personal autorizado

Todos los sistemas permiten al personal autorizado editar el diseño de personalización mediante el editor de diseño. Con el editor de diseño es posible añadir gráficos o texto

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

EMDOC
CONSORCIO

adicionales. El editor de diseño láser es una potente herramienta para la disposición de todos los elementos en la tarjeta u otros objetos imprimibles. Permite añadir objetos (tipos de campo) como texto, incluidos caracteres alfanuméricos, imágenes, códigos de barras (1D y 2D), objetos gráficos estándar (círculos, rectángulos, líneas) al documento y, por supuesto, organizar la posición/ubicación de estos elementos en el documento.
Las propiedades de cada campo pueden modificarse en relación con los tipos de letra, tamaños de letra, tamaños de imagen y posiciones del campo de grabado.
Además, el sistema permite imprimir todas las fuentes True Type de Windows y fuentes personalizadas en el formato True Type de Windows.



EMDOC CONSORCIO

1.5. Personalización

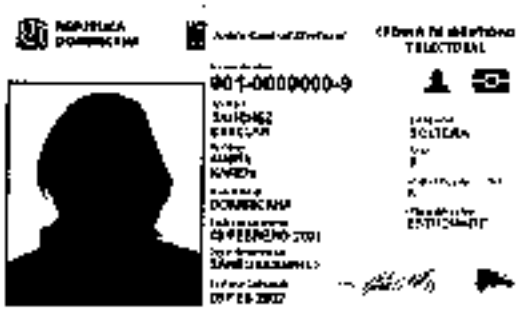
La eficiencia de producción de los sistemas de máquinas de impresión propuestos será superior al 90% siempre:

- los lotes de producción adecuados se transfieren a las máquinas de impresión para que, cuando se midan en consecuencia, no se produzcan interrupciones debidas a la selección y activación de los trabajos
- el sistema lo maneja personal cualificado y está en buenas condiciones técnicas
- los módulos de entrada se rellenan con el material necesario
- suministro ininterrumpido de insumos y sin interrupción de la producción
- disponibilidad permanente y estable de los medios técnicos y las condiciones del entorno de producción

1.6. Personalización según el formato y el diseño solicitados

Las máquinas de impresión de personalización permitirán personalizar el documento de acuerdo con las ilustraciones siguientes. La disposición final de la Capacitación personalizada se acordará teniendo en cuenta la viabilidad técnica y en consulta con el cliente.

1.6.1. Formato (Lay out) de las tarjetas ICN

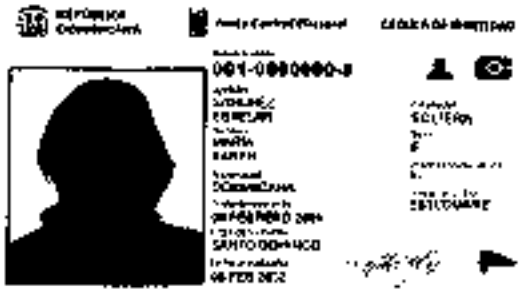


Anverso de la tarjeta: CIE



Reverso de la tarjeta: CIE

1.6.2. Formato (Lay out) de las tarjetas CI



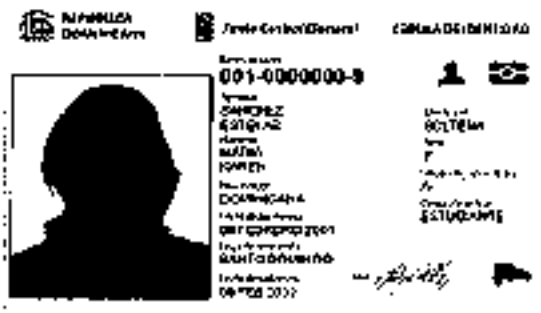
Anverso de la tarjeta: CI Policía



Reverso de la tarjeta: CI Policía

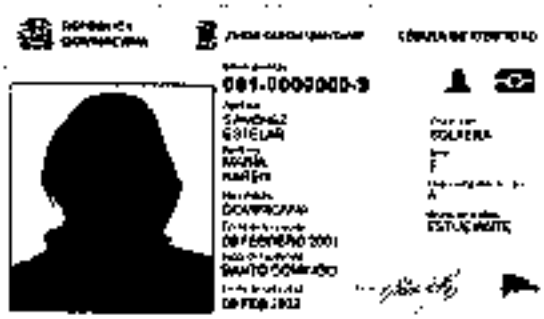
CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

EMDOC
CONSORCIO



Anverso de la tarjeta: CI Militar

Reverso de la tarjeta: CI Militar



Anverso de la tarjeta: CI Menor

Anverso de la tarjeta: CI Menor



Anverso de la tarjeta: CI Extranjero

Anverso de la tarjeta: CI Extranjero

1.7. Sistema de desarrollo de software

Para el desarrollo de aplicaciones de personalización de chips, se proporciona el Sistema de Desarrollo de Software para MCES.

El Sistema de Desarrollo de Software para MCES es un paquete que proporciona las herramientas y bibliotecas para un desarrollo fácil e independiente de extensiones MCES para asegurar una reacción instantánea a los cambios de sistema y requisitos.

Sistema de desarrollo de software MCES (SDK, APIS)

El Sistema de Desarrollo de Software MCES soporta el desarrollo y prueba de extensiones del Módulo de Proceso MCES como aplicaciones de personalización de chips y extensiones de interfaz MCES, como MCES Monitoring DLLs, MCES Exchange DLLs, MCES DataMatching DLLs, MCES Reporting DLLs, MCES Pre- y Post-Process DLLs, aplicaciones de importación de datos MCES así como XML Jobs.

Características

- Desarrollo independiente
  - Ampliaciones del módulo de procesos del MCES
  - Ampliación de interfaces
- Reacción instantánea a los cambios en el sistema y los requisitos
- Depuración y pruebas sencillas

Productos - Software

- Biblioteca básica del MCES
- Biblioteca de informes MCES
- Plantillas MCES
  - Plugins MCES (DLL de supervisión, DLL de intercambio, DLL de informes, DLL de comparación de datos, DLL de preprocesamiento y postprocesamiento, DLL de adquisición de datos)
- Entorno MCES para pruebas
- Scripts de bases de datos SQL
- Herramientas de prueba y configuración
- Documentación

La estación de trabajo de desarrollo del MCES es un ordenador portátil o un PC en el que se instalará el sistema de desarrollo de software de MCES. Está equipado con el sistema operativo Microsoft Windows® (Windows10), Microsoft SQL Server® y Microsoft Visual Studio®.

Características

- Preparar la configuración de los trabajos
- Crear archivos de diseño

Productos - Hardware

- Sistema-PC:
  - Portátil - chipset Intel® (por defecto)
  - Controladores y documentación

CONSORCIO EMDOC y EMDOC CONSORCIO Santo Domingo, R.D.

- Ejecute procedimientos de prueba fuera de línea sin afectar a la producción
- Conectarse al software de gestión de la producción para realizar pruebas
- Validación de parches, actualizaciones y mejoras
- Instalación conforme a los sistemas de personalización existentes o futuros
- Nuevos sistemas de personalización capaces de integrarse

Productos - Software

- **Sistema operativo:** Windows 10
- **Servidor SQL:** Microsoft SQL Server
- **Entorno de desarrollo:** Microsoft Visual Studio
- Entorno MCES II preinstalado:
  - Interfaz gráfica de usuario de Mühlbauer
  - Diseñador de productos MCES
  - Base de datos MCES
  - Aplicación XMLDataAcquisition
  - Herramientas MCES
  - Software y archivos relacionados con el cliente (software desarrollado para el cliente)
- Documentación MCES

Paquete de ampliación Codificación de chips - MB 1301 (TCP/IP)
La Extensión de Codificación de Chip MB1301 es un paquete de extensión para el Kit de Desarrollo de Software MCES. Proporciona el software (plantillas, bibliotecas) y hardware para un desarrollo fácil e independiente de aplicaciones de codificación de chip MCES (Chip-Coding-DLLs) para la codificación de tarjetas inteligentes con o sin interfaz de contacto con el software MCES Machine Personalization Management System.

Características

- Desarrollo independiente
  - Módulos de ampliación de codificación de chips (DLL) para chips con o sin interfaz de contacto
- Reacción instantánea a los cambios en el sistema y los requisitos
- Depuración y pruebas sencillas
- Lector de tarjetas inteligentes MB1301

Requisitos del pliego de condiciones

- Kit de desarrollo de software MCES
- Interfaz Ethernet
- Nivel de conocimientos
  - Sistema operativo Windows (Microsoft Windows®)
  - VisualStudio, C#, diseño orientado a objetos
  - Lenguaje extensible de marcas (XML)/lenguaje extensible de hojas de estilo (XSL)
  - Base de datos relacional, lenguaje de consulta estructurado (SQL)
  - Conocimientos de codificación de tarjetas inteligentes/chips
  - Conceptos básicos de criptografía

Hardware

- Lector de tarjetas inteligentes:
  - MB1301 Lector de codificación por chip con y sin contacto (TCP/IP)

Software

- Plantillas MCES
  - Codificación de chips DLL
  - Lector DLL
- Herramientas de prueba y configuración
- Documentación

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

EMDOC
CONSORCIO

ENTREGABLES MÁQUINAS DE IMPRESIÓN

PARA LA CONTRATACIÓN DE LA EMPRESA QUE SE ENCARGARÁ DE SUPLIR LOS EQUIPOS, MATERIALES Y SERVICIOS PARA LA IMPRESIÓN DE LA CÉDULA DE IDENTIDAD Y ELECTORAL (CIE) Y CÉDULA DE IDENTIDAD (CI)

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

Entregables

Posición	Breve descripción de la configuración propuesta	Unidades	Comentario
1	**Sistemas de máquina de impresión de personalización incl.:** • Módulo de entrada de tarjetas • de chips • Sistema láser • Sistema de control de tarjetas • Módulo de salida incl. compartimento de rechazo Otros equipos incluidos: • PC interno • Sistema de alimentación ininterrumpida • USB-Módulo de alta seguridad (HSM) Software de control de máquina de impresión • Módulo de importación de datos • Base de datos de máquina de impresión • Herramienta de registro • Preparación de datos • Firma de documentos • Sistema de gestión de claves • Informes Garantía • 2 años a partir de la fecha de entrega	214	**Mühlbauer CLP 60** **Mühlbauer MCES**

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, RD

2	**Sistemas de máquina de impresiónes de personalización incluye:** • Módulo alimentador de entrada de tarjetas • Codificación de chips • Sistema láser • Sistema de control de tarjetas • Módulo de salida incluye compartimento de rechazo Otros equipos incluidos: • PC interno • Sistema de alimentación ininterrumpida • USB-Módulo de alta seguridad (HSM) Software de control de máquina de impresión • Módulo de importación de datos • Base de datos de máquina de impresión • Herramienta de registro • Preparación de datos • Firma de documentos • Sistema de gestión de claves • Informes Garantía • 2 años a partir de la fecha de entrega	10	**Mühlbauer CLP 60** **Mühlbauer MCES**
3	**Paquete Repuestos**	1	
4	**Suministro de SDK**	1	
5	**Accesorios: Dispositivo láser de verificación de la calidad (Densitómetro de color)**	5	

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

80

EMDOC
CONSORCIO

ITEM III. Especificaciones Técnicas de las PKI CA y PKI Identidad Física y Digital

PARA LA CONTRATACIÓN DE LA EMPRESA QUE SE ENCARGARÁ DE SUPLIR LOS EQUIPOS, MATERIALES Y SERVICIOS PARA LA IMPRESIÓN DE LA CÉDULA DE IDENTIDAD Y ELECTORAL (CIE) Y CÉDULA DE IDENTIDAD (CI)

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

EMDOC
CONSORCIO

CONTENIDO

1. Especificaciones de la Infraestructura de Llave Pública (PKI CA) 4
1.1 Propósito 4
1.2 Objetivo general 4
1.3 Objetivos principales 4
1.4 Componentes y servicios incluidos 5
1.4.1 Licencias a perpetuidad 5
1.4.2 Equipos criptográficos (HSMs UTIMACO): 7
1.4.3 Servicios profesionales 7
1.5 Propuesta de solución 8
1.6 Funcionalidad de Firma Electrónica mediante la PKI propuesta 9
1.7 Características de la PKI propuesta 11
1.8 Otras consideraciones para la CSCA 13
1.9 Descripción funcional de los componentes de la PKI 15
1.9.1 Arquitectura de la PKI (conceptual) 15
1.10 Autoridad Certificadora Raíz 19
1.10.1 Funcionalidad: 19
1.10.2 Beneficios: 19
1.11 Autoridad Certificadora Subordinada (operativa o ciudadana) 20
1.11.1 Funcionalidad: 20
1.11.2 Beneficios: 20
1.12 Portal de Certificación (enrolamiento) empleando las cédulas de identidad 21
1.12.1 Funcionalidad: 21
1.12.2 Beneficios: 21
1.13 Portal Web de Firma 22
1.13.1 Funcionalidad: 22
1.13.2 Beneficios: 22
1.14 PKI (Infraestructura de Llave Pública) 23
1.14.1 Componentes de la Infraestructura de Llave Pública (PKI): 23
1.14.2 Beneficios Generales de la PKI: 24
1.15 Integración de la firma digital con las aplicaciones de la ICE empleando las cédulas de identidad (smartcards con chip) 24
1.15.1 Proceso de Integración de la Firma Digital con Llaves en Smartcard: 25
1.16 Mantenimiento del licenciamiento de la PKI 26
1.17 Servicios de soporte técnico 7x24 de los productos y componentes 27
1.17.1 Soporte Técnico del HSM 28
1.18 Duración del Servicio 28
1.19 Lugar y Programa de Suministros 28
1.20 Entregables del Proyecto 28
1.21 Anexos a Solución PKI 31
1.21.1 Descripción técnica funcional de productos PKI 31
Descripción técnica autoridad certificadora (SeguriServer) *31*
1.21.2 Descripción técnica de Autoridad Emisora de Estampas de Tiempo (TSA - SeguriNotary) 40
1.21.3 Descripción técnica de Motor de Firma Electrónica (SeguriSign) 42
1.21.4 Descripción técnica de Módulo CryptoServer CP5 SE 500 de Utimaco 47
1.21.5 Descripción técnica de Módulo CryptoServer CP5 SE 12 de Utimaco 50
2 Especificaciones de la (PKI) para la emisión de la identidad física y digital (CI/CIE) 53
Especificaciones de la (PKI) para la emisión de la identidad física y digital (CI/CIE) 53
Requisitos del sistema 54
Integración del sistema 55

2.3.1 AUTENTICACIÓN PASIVA PKI 55
2.3.2 SISTEMA PKI DE CONTROL DE ACCESO AMPLIADO 56
2.3.3 FIRMA DIGITAL PKI 57
2.3.4 ISO 18013-5 PKI 58
2.4 INTERFACES DEL SISTEMA 59
2.4.1 AUTORIDAD DE CERTIFICACIÓN CON FIRMA DE PAÍS (CSCA) 59
2.4.2 AUTORIDAD DE CERTIFICACIÓN VERIFICADORA DE PAÍSES (CVCA) 59
2.4.3 FIRMA DIGITAL PKI 60
2.4.4 AUTORIDAD EMISORA AUTORIDAD DE CERTIFICACIÓN (IACA) 60
2.5 FUNCIONALIDAD 61
2.5.1 AUTORIDAD DE CERTIFICACIÓN CON FIRMA DE PAÍS (CSCA) 61
2.5.2 AUTORIDAD DE CERTIFICACIÓN DE VERIFICACIÓN DE PAÍS (CVCA) 61
2.5.3 FIRMA DIGITAL PKI 62
2.5.4 AUTORIDAD EMISORA AUTORIDAD DE CERTIFICACIÓN (IACA) 63
2.6 REQUISITOS NO FUNCIONALES 63
2.6.1 DISPONIBILIDAD DEL SISTEMA 63
2.6.2 SEGURIDAD DEL SISTEMA 64
2.6.3 DESPLIEGUE DEL SISTEMA 64
2.7 HARDWARE Y SOFTWARE DEL SISTEMA PKI 65
REFERENCIAS: 66

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

1. Especificaciones de la infraestructura de llave pública (PKI CA)

La **Infraestructura de Llave Pública** (PKI, por sus siglas en ingles *"Public Key Infrastructure"*) será la utilizada para garantizar la autenticidad, integridad y no repudio de documentos electrónicos mediante la firma digital. En la funcionalidad de firma electrónica para los ciudadanos se ha especificado que se requiere que dicha firma sea cargada al chip de la cedula de identidad y que se suministre una aplicación que maneje todo el ciclo de vida de dicha firma, es decir renovación, renovación, sellado de tiempo, etc. La **Infraestructura de Llave Pública** constará con su propia cadena de confianza completa, estando en línea o fuera de línea. Entre otras funcionalidades, permitirá a los ciudadanos la firma de documentos.

1.1 Propósito

Implementar una PKI para que la JCE esté en condiciones de gestionar todo el ciclo de vida de los certificados digitales que serán resguardados en la cédula de identidad que les será entregada a cada ciudadano. Mediante dichos certificados se dan elementos para verificar la autenticidad e integridad de los documentos de identidad ciudadana y al mismo tiempo los ciudadanos estarían en condiciones de firmar electrónicamente en procesos que implemente para tal fin el gobierno de la República Dominicana. Se incluye en este alcance los servicios profesionales para la integración de la firma electrónica en servicios públicos que señale la JCE, como por ejemplo en los ámbitos: electorales, del registro civil así se beneficien de los servicios de firma electrónica que facilitan validar la identidad de las personas. La interoperabilidad de la PKI se logra mediante APIs y Servicios web con tecnología API REST para verificar que los documentos sean auténticos e íntegros.

1.2 Objetivo general

Suplir los equipos, materiales y servicios para implementar una PKI que interoperará con la nueva "Cédula de Identidad y Electoral y Cédula de Identidad" para Incorporar nuevas tecnologías que aporten mayores niveles de seguridad, para de esa manera, dar seguimiento a la estrategia diseñada por las actuales autoridades de la Junta Central Electoral, vinculada a la modernización y mejoramiento de los servicios que ofrece a la ciudadanía, relacionados con la función electoral y las atribuciones que la Carta Magna le otorga, en materia del Registro Civil y de la Cédula de Identidad.

1.3 Objetivos principales

Son los siguientes:

- Implementar una PKI con redundancia en un sitio principal (producción) con el fin de tener continuidad en la operación.
- Implementar una PKI en un sitio alterno y alejado geográficamente del sitio principal, con el fin de reforzar el punto anterior, y que, en caso de algún contratiempo que interrumpa la operación del sitio principal se active este sitio alterno al que se denomina DRP (Disaster Recovery Plan).
- Implementar una PKI en un ambiente de pruebas, a fin de que el equipo de la JCE disponga de lo necesario para que pueda integrar la firma electrónica en todos

aquellos procesos y/o aplicaciones que el gobierno considere y que se traduzca en mejores servicios para la ciudadanía.

- Crear para la JCE su propia Autoridad Certificadora (AC), mediante la cual podrá controlar el ciclo de vida de los certificados digitales, esto coadyuva en garantizar la autenticidad y seguridad del documento de identidad. Se contempla crear una Autoridad Certificadora Raíz y una Autoridad Subordinada Operativa.
- Brindar los conocimientos a la JCE para que quede documentada el cómo se regirá la operación cotidiana de la AC.
- Implementar los componentes que acompañarán a la AC que permiten crear la PKI: una TSA (TimeStamp Authority) y un Motor de Firma.
- Realizar los servicios profesionales de nuestro personal especializado. En particular el acompañamiento del nacimiento operativo de la AC de la JCE, y en general puesta a punto, capacitación y arranque de la operación de la PKI, así como los servicios de soporte y mantenimiento de todos los componentes en los tres ambientes mencionados. En la siguiente sección (Componentes y servicios incluidos) se detallan estos.

1.4 Componentes y servicios incluidos

La presente propuesta considera la entrega de licencias, equipos criptográficos y servicios profesionales, para poner en operación y a punto una PKI con Autoridad Certificadora (AC), dentro de los plazos que señala el pliego petitorio.

Los componentes y servicios de la solución son los siguientes:

1.4.1 Licencias a perpetuidad

- SeguriServer (Autoridad Certificadora)
  - Ambiente Productivo
    - 1 instancia de servicio (1 Servidor [AC Raíz])
    - 2 instancias de servicio (2 Servidores [Activo - Pasivo]) para AC subordinada (operativa)
    - Licenciamiento cliente x procesador
  - Ambiente DRP
    - 1 instancia de servicio (1 Servidor) para AC Raíz
    - 1 instancia de servicio (1 Servidor) para AC subordinada (operativa)
    - Licenciamiento cliente x procesador
  - Ambiente Desarrollo
    - 1 instancia de servicio (1 Servidor)
- SeguriNotary (TSA - Autoridad De Sellos de Tiempo)
  - Ambiente Productivo
    - 2 instancias de servicio (2 Servidores [Activo - Pasivo])
    - Licenciamiento cliente x procesador
  - Ambiente DRP
    - 1 instancia de servicio (1 Servidor)
    - Licenciamiento cliente x procesador
  - Ambiente Desarrollo
    - 1 instancia de servicio (1 Servidor)
- SeguriSign (Motor de Firma Electrónica)

CONSORCIO EMDOC Santo Domingo, R.D.

- Ambiente Productivo
  - 2 instancias de servicio (2 Servidores [Activo - Pasivo])
  - Licenciamiento cliente x procesador
- Ambiente DRP
  - 1 instancia de servicio (1 Servidor)
  - Licenciamiento cliente x procesador
- Ambiente Desarrollo
  - 1 instancia de servicio (1 Servidor)

- Portal de Certificación (enrolamiento)
  - Ambiente Productivo
    - 2 instancias de servicio (2 Servidores [Activo - Pasivo])
    - Licenciamiento cliente x procesador
  - Ambiente DRP
    - 1 instancia de servicio (1 Servidor)
    - Licenciamiento cliente x procesador
  - Ambiente Desarrollo
    - 1 instancia de servicio (1 Servidor)
- Vertical de firma (incluye portales de: Administración, Agente y Firma)
  - Ambiente Productivo
    - 2 instancias de servicio (2 Servidores [Activo - Pasivo])
    - Licenciamiento cliente x procesador
  - Ambiente DRP
    - 1 instancia de servicio (1 Servidor)
    - Licenciamiento cliente x procesador
  - Ambiente Desarrollo
    - 1 instancia de servicio (1 Servidor)
- API
  - API con soporte a PKCS#11
    - Licencia corporativa para la JCE.

Las buenas prácticas indican estos vencimientos:

- Certificados de CA Raíz: Suelen tener una duración más larga (10-20 años) debido a la complejidad y la amplia distribución de la infraestructura que dependen de ellos.
- Certificados Intermedios: Duraciones moderadas (5-10 años) para asegurar un equilibrio entre seguridad y operatividad. Permiten un ciclo de renovación menos frecuente que minimiza las interrupciones.
- Certificados de Usuario Final y Servidor: Duraciones cortas (1-3 años) para maximizar la seguridad y la flexibilidad en la gestión. Son más fáciles de renovar y revocar en caso de compromisos.
- Se debe proveer la funcionalidad de revocación de certificados y la funcionalidad de sello de tiempo (Time Stamp).
- El vencimiento del certificado digital será estipulado dando cumpliento con la Ley de Comercio Electronico nacional y su reglamento

CONSORCIO EMDOC Santo Domingo R.D.

EMDOC CONSORCIO

1.4.2 Equipos criptográficos (HSMs UTIMACO):

- 3 módulos de seguridad criptográfica CryptoServer CP5 Se 500 de Utimaco, con cumplimiento Common Criteria, eIDAS y FIPS 140-2 Nivel 3 o superior, que cumplen con las características descritas en el apartado Hardware Criptográfico, considerar impuestos, 2 equipos serán para ambiente productivo y 1 equipo para ambiente DRP.
- 2 módulos de seguridad criptográfica CryptoServer CP5 Se 12, con cumplimiento Common Criteria, eIDAS y FIPS 140-2 Nivel 3 o superior, que cumplen con las caracteristicas descritas en el apartado Hardware Criptográfico, considerar impuestos, 1 equipo será para ambiente productivo y 1 equipo para ambiente DRP.
- 5 pólizas de Pólizas de Mantenimiento Premium para los 5 equipos: 3 CryptoServer CP5 Se 500 y 2 CryptoServer CP5 Se 12, con vigencia de 12 meses a partir de la firma del contrato.

1.4.3 Servicios profesionales

- Instalación y configuración de la solución que se proponga para los tres ambientes:
  - Producción en alta disponibilidad.
  - DRP en disponibilidad simple.
  - Desarrollo en disponibilidad simple.
- Asistencia Técnica en Normatividad de la Autoridad Certificadora para la generación del sustento legal de la Autoridad Certificadora de la JCE. Estos servicios brindan todo lo necesario para acompañar a la JCE en el nacimiento operativo de su AC y se genera la documentación que reglamenta la operación de la misma. Incluye las actividades de realizar la ceremonia de atestiguamiento y la generación del script para llevar a cabo la ceremonia.
- Asistencia técnica de integración de 1(una) aplicación o un máximo de 40 horas para a la integración de firma digital a una aplicación o proceso propietaria que designe la JCE.
- Capacitación (transferencia de conocimientos). Para el personal de la JCE, la capacitación va dirigida tanto a desarrolladores como al personal designado por la JCE que operará la solución tecnológica.
- Pólizas de soporte técnico 7x24 y mantenimiento de todos los componentes de software de la PKI propuesta (Licenciamiento a perpetuidad) con vigencia por la duración del contrato.
- Mantenimiento premium para los equipos criptográficos de la marca Utimaco por el fabricante

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

- Servicios de desarrollo para ajustar componentes especializados que permitan integrar la firma electrónica con el uso de las cédulas. Estos componentes son los siguientes:

  - SeguriLib/Librería Criptográfica
  - SeguriServer
  - SeguriSign Core
  - Bibliotecas Propósito General
  - Extensión Navegador de Internet (Browser)
  - Portal Firma
  - Portal Administración Certificados
  - Documentación
  - API criptográfica para soportar PKCS#11

Las funcionalidades a habilitar en los componentes previos son:

- Soportar HSM de UTIMACO para los productos de la AC Raiz y AC Subordinada.
- Integración de PKCS11 de UTIMACO en software de Autoridad Certificadora
- Adecuaciones al software de las Autoridades Certificadoras (AC) , al Motor de firma, modificar los Web Services de generación de PDF con soporte a ECC
- Modificaciones al Portal de Admon de Certificados para recibir ECC para certificados de AC con ECC
- Consumir el PKCS11 para librerías de Firma y generación de llaves para integrar el Middleware que entregará Veridos Alemania
- Soporte de extensión Chrome para generación de llaves en la tarjeta, asociar el certificado instalado en la tarjeta y generar la firma
- Portal de Firma la nueva extensión de Chrome que incluye el middleware de Veridos
- Portal de Administración de Certificados para habilitar la interoperabilidad con soporte a las tarjetas de República Dominicana
- API para integración de firma en las Aplicaciones del cliente para las nuevas tarjetas

1.5 Propuesta de solución

Mediante la implementación de la PKI se logra lo siguiente:

- Autenticación Segura: La PKI permite que cada cédula emitida tenga un certificado digital único que autentica la identidad del portador de manera segura, haciendo uso de la criptografía de clave pública.

- Integridad de los Datos: Asegura que la información contenida en las cédulas no pueda ser alterada sin detección, mediante firmas digitales.
- Confianza en el Sistema: Al implementar una PKI, la Junta Central Electoral puede garantizar a los ciudadanos y a las entidades que requieren verificación de identidad, que el sistema es robusto y seguro.

Otros objetivos que nuestra solución cumple, son:

a) Actualiza la Información Personal y Biométrica:

- Certificación de la Autenticidad: Los certificados digitales gestionados por la PKI pueden ser utilizados para verificar que la actualización de los datos proviene de una fuente auténtica y autorizada.
- Control de Acceso Seguro: La PKI permite establecer controles de acceso basados en certificados digitales, asegurando que solo personal autorizado pueda acceder o modificar los datos biométricos y personales.

b) Garantiza la Autenticidad y Seguridad del Documento:

- Prevención de Fraudes: La PKI proporciona un mecanismo para que cada documento de identidad emitido sea único y verificable, lo que complica significativamente la falsificación y el uso fraudulento de documentos.
- Firma Digital: Los documentos pueden ser firmados digitalmente para verificar su autenticidad y verificar que no han sido modificados desde su emisión.

c) Facilita el Acceso a Servicios Mediante un Ecosistema Interoperable:

- Interoperabilidad: La PKI, al ser un estándar reconocido y ampliamente utilizado para la seguridad en las comunicaciones digitales, facilita la interoperabilidad entre diferentes sistemas y plataformas que utilizan API REST y otras tecnologías.
- Gestión del Ciclo de Vida de los Certificados: La PKI no solo emite certificados, sino que también los revoca y los renueva, gestionando todo el ciclo de vida de los certificados digitales, lo que es crucial para mantener la seguridad del sistema en el tiempo.

1.6 Funcionalidad de Firma Electrónica mediante la PKI propuesta

La PKI propuesta es totalmente compatible con la PKI ICAO de las cédulas para establecer un SOD activado en los datos del chip. Lo anterior lo logramos debido a que nuestra PKI es capaz de generar, gestionar y validar las firmas digitales y certificados que son utilizados para proteger y verificar la autenticidad de los datos almacenados en el chip de un documento electrónico, conforme a los estándares de la OACI. Esto asegura

que los datos biométricos y personales en el chip están protegidos contra modificaciones no autorizadas y pueden ser verificados de manera confiable a través de fronteras internacionales.

El acceso a la tarjeta está protegido mediante el uso de un Número de Identificación Personal (PIN) y una Clave Personal de Desbloqueo (PUK) para proteger el acceso a una tarjeta con chip es un enfoque estándar en la seguridad de tarjetas inteligentes.

Se soportan algoritmos de firma como RSA y ECDSA, asimismo, claves en formato CRT (Chinese Reminder Theorem) y en formato normal. Para el caso de RSA, para cada par de llaves, se generan números primos pseudoaleatorios p y q, dependiendo del tamaño de las claves se varía su tamaño, para más información ver la sección de Anexos [ver sección "Descripción técnica autoridad " (SeguriServer) y sección "Descripción técnica de Motor de Firma Electrónica" (SeguriSign)].

La PKI propuesta implementa PKCS#15, es decir, implementa el formato y organización específicos para los archivos de datos almacenados en tarjetas inteligentes que usan tecnología de chip integrado.

Se proveerán como parte de la solución, tarjetas con memoria suficiente para almacenar hasta 4 certificados, con sus correspondientes claves, incluyendo el caso de claves RSA 4096.

Cuando se generen los certificados digitales en las cédulas se soporta la autenticación de la información intercambiada; incorporando HMAC según ANSI X9.19 y DES. Sin embargo, proponemos el uso de AES en lugar de DES, dado que DES ya no es seguro.

El establecimiento del protocolo para generar claves de sesión basado en el esquema propuesto en ISO/IEC 9798-3 Authentication SASL Mechanism se plantea del siguiente modo, asumiendo que ya se tienen los certificados en las cédulas de identidad:

Intercambio de Claves y Autenticación

- Intercambio de Claves Públicas: Las entidades intercambian sus claves públicas, es decir sus certificados digitales.
- Generación de Claves de Sesión: Cada parte genera una clave de sesión, que puede ser una clave simétrica temporal para cifrar la comunicación durante una sesión.

Autenticación Utilizando Firmas Digitales

- Firma de la Clave de Sesión: Cada parte firma la clave de sesión generada utilizando su clave privada.
- Envío de la Clave de Sesión Firmada: La clave de sesión firmada se envía a la otra entidad junto con el certificado digital del emisor.

- Verificación de la Firma: Al recibir la clave de sesión firmada, la entidad receptora utiliza la clave pública del emisor, extraída de su certificado digital, para verificar la firma. Esto asegura la autenticidad de la clave de sesión y confirma la identidad del emisor.

Establecimiento de la Comunicación Segura

Una vez que ambas partes han verificado las claves de sesión:

- Cifrado de Comunicaciones: Utiliza las claves de sesión para cifrar y descifrar la comunicación entre las entidades, asegurando la confidencialidad y la integridad de los datos intercambiados.
- Re-autenticación: Pueden implementarse mecanismos de re-autenticación periódica para mantener la seguridad de la comunicación a lo largo del tiempo.

Mediante el empleo de criptografía de curvas elípticas (ECC), se generan la clave privada y de esta se deriva la correspondiente clave pública. el estándar ANSI X9.63 especifica cómo dos partes pueden cooperar para crear una clave compartida que puede ser usada para cifrar comunicaciones subsecuentes. Esta cooperación bien puede realizarse usando RSA o ECC.

1.7 Características de la PKI propuesta

Para mayor detalle de toda la funcionalidad de la PKI ofertada ver en la sección Anexos, (ver sección "Descripción técnica funcional de productos PKI"). En este apartado listamos algunos aspectos funcionales de la misma.

Mediante el uso de los certificados emitidos por el servidor de la Autoridad Certificadora (AC), los sellos de tiempo emitidos por el componente SeguriNotary (TSA) para dotar de certeza respecto al momento en que se plasma una firma y el componente SeguriSign (Motor de firma electrónica) que permite el uso de los del lado cliente (usuario) para que se ejecute la firma, se proveen todos los beneficios que otorga la firma electrónica a los documentos:

- **Integridad** (el documento firmado no ha sufrido alteraciones),
- **Autenticación** (quién firmó) y
- **No repudio** (no se puede negar haber firmado).

La PKI implementada gestiona el ciclo de vida de los certificados: emisión, revocación y renovación de los mismos que se utilizarán para firmar electrónicamente las tarjetas electrónicas (CSCA) y para verificar tarjetas electrónicas (CVCA). Al mismo tiempo la PKI permite las verificaciones de identidad que menciona el estándar ISO 18013-5.

La PKI es compatible con Common Criteria, en el caso del equipo criptográfico (HSM) cumple con las certificaciones de eIDAS, Common Criteria, FIPS 140-2 N3, entre otras especificaciones (Para más detalles ver en la sección de Anexos, la destinada a la

descripción técnica de Módulo nShield). El HSM resguardará las claves de la Autoridad Certificadora de la JCE, con las cuales se firmarán los certificados digitales que estarán en las cédulas de identidad.

En la sección de Anexos podrá consultarse todos los aspectos relacionados al software y hardware necesarios para dejar implementada la PKI que se propone. Por ejemplo, toda la gestión de las firmas la llevará SeguriSign, asimismo todo el ciclo de vida de los certificados lo cubre SeguriServer, en particular las listas de certificados revocados (CRL), conforme a las especificaciones funcionales de la OACI.

SeguriServer (Autoridad Certificadora de la PKI):

- Permite firmar certificados para entidades gubernamentales o documentos de importancia nacional.
- Utiliza algoritmos criptográficos actuales y almacenará las claves privadas en un HSM de cualquier fabricante, en particular el que proponemos es de la marca Utimaco.
- Permite verificar certificados revocados mediante la publicación periódica de una lista de revocación de certificados (ICAO 9303).
- Puede trabajar en un entorno sin conexión.
- Puede utilizar autenticación multifactorial para el inicio de sesión en la interfaz de administración, por ejemplo, la combinación de contraseña y el uso de certificados digitales.
- Puede firmar un VDS (Visible Digital Seal), que es una especie de "sello digital visible" que se utiliza en documentos de viaje y otros documentos de identidad. SeguriServer al firmar estos sellos, se asegura que la entidad que firma el VDS es legítima y que los datos contenidos en el sello son auténticos y no han sido alterados desde su emisión.
- Permite asegurar que los certificados incluidos en la lista maestra sean legítimos y estén bien gestionados, lo que incluye la emisión, renovación y revocación de los mismos.
- Puede ser configurado para que firme (Document Signer) documentos digitales de manera masiva, por ejemplo, los certificados de de las cédulas de identidad o los VDS. Lo anterior con las llaves estando resguardadas en un HSM para el control de la seguridad.
- El SOD (Signed Object Directory) es un componente crucial en los documentos de viaje electrónicos. Contiene datos digitales críticos como información biográfica y biométrica, que pueden ser firmados digitalmente por el componente SeguriServer (Document Signer).

- El componente SeguriServer posee una capa de Servicios web tipo REST para la firma del SOD.
- Utiliza algoritmos criptográficos actuales y almacenará las claves privadas en un HSM de cualquier fabricante, en particular de un HSM Utimaco propuesto.
- Permite el control de acceso en la interfaz de administración mediante el uso de la autenticación multifactorial, dando aviso antes de que expire el tiempo de uso de la clave del certificado actualmente utilizado.
- Se pueden configurar un par de claves destinadas resguardas en el HSM para un DS exclusivo que firme los DTC (Digital Travel Credential. Estándar ICAO de documento de viaje en móvil) para la aplicación Tarjeta Digital de la JCE. Se requerirá implementar una interfaz que permita acceder al sistema back-end de la JCE.

1.8 Otras consideraciones para la CSCA

EMDOC implementará una CA con especificaciones y un marco que cumplan con el Documento 9303 de la OACI vigente sobre el esquema de Firmas Digitales PKI propuesto para autenticar la tarjeta electrónica que ofrece acceso de sólo lectura de Chip de Circuito Integrado (IC).

EMDOC proveerá el licenciamiento, equipos criptográficos y servicios profesionales para instalar y configurar la PKI de la JCE, en particular la CA para generar conjuntos de claves para diferentes períodos de tiempo que se utilizarán para computar las Firmas Digitales que se aplicarán para la firma de los Certificados. La arquitectura que se propone es multicapa, siendo los datos y equipos criptográficos situados en la red interna de la JCE con todas las medidas de seguridad apropiadas, tanto físicas como lógicas. La ubicación de los sistemas o instalaciones propuestos será proporcionada por la JCE.

Los certificados de CA de firma del país se generarán en una infraestructura de CA sin conexión, altamente protegida. La solución cumple con estándares internacionales de criptografía y de las mejores prácticas de arquitectura de soluciones. Los certificados digitales están codificados de acuerdo al estándar X509. Asimismo, como parte de la solución se considera la implementación, configuración y puesta en operación de equipos criptográficos HSM, certificados con FIPS 140-2 N3, que serán instalados en las instalaciones de la JCE.

Toda la infraestructura adicional (racks, cableado, etc.), será provista con las características señaladas en las secciones: 6.1.4 Descripción técnica de Módulo CryptoServer CP5 SE 500 Utimaco y 5.1.7 Descripción técnica de Módulo CryptoServer CP5 SE 12 de Utimaco.

El certificado DS será emitido por la CSCA (SeguriServer). Para el caso de procesos de firma masiva, la PKI (SeguriServer) será responsable de la generación de claves/certificados de seguridad requeridos, no así las de los ciudadanos, serán estos

los que en completa privacidad generarán su par de claves y requerimiento de certificación, siendo la CSCA la encarga de emitir el certificado correspondiente mediante un agente certificador.

Tola la infraestructura propuesta de la PKI de la JCE se prevé este actualizada anualmente y garantizando su conformidad cuando sea requerida por una puesta al día de las normas y especificaciones contenidas en el Documento 9303, o cuando sea requerido por la JCE.

Especificaciones técnicas tarjeta de identidad digital y la Autoridad Certificadora

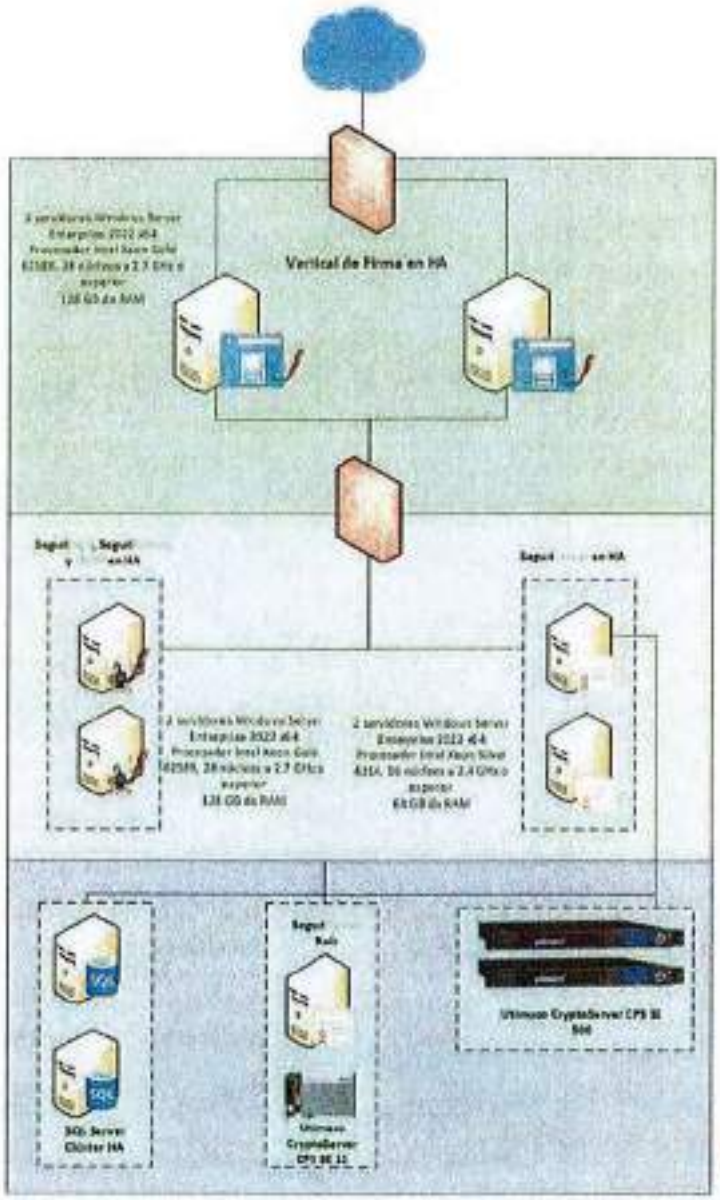
La tarjeta digital podrá ofrecer (si las leyes lo permiten) las mismas garantías jurídicas al titular que el CEI o CI. Los datos entregados y asociados a la tarjeta misma, al dueño de la tarjeta (ciudadano) podrán ser firmados electrónicamente. Esta firma electrónica certificada de los datos permitirá que terceros puedan validar la integridad y procedencia de los datos que presenta el ciudadano. Los datos entregados serán firmados electrónicamente con las claves criptográficas de la JCE, que estarán resguardadas en el HSM. Esta firma electrónica certificada de los datos permitirá que terceros puedan validar la integridad y procedencia de los datos que presenta el ciudadano, tanto la firma de los datos como la validación de estos, se realizará usando los certificados electrónicos administrados por la CA de la JCE, con la figura de Autoridad Certificadora descrita en el apartado Infraestructura de clave pública (PKI).

CONSORCIO EMDOC Santo Domingo, R.D.

1.9 Descripción funcional de los componentes de la PKI

1.9.1 Arquitectura de la PKI (conceptual)

Arquitectura para el ambiente de producción



CONSORCIO EMDOC
EMDOC CONSORCIO
Santo Domingo, RD

Se provee redundancia en todos los componentes con el objeto de tener continuidad en la operación, el esquema será de conmutación por falla (failover) o por balanceo de cargas. Para este dispondremos de un balanceadora carga (ver descripción de la infraestructura).

Asimismo, puede observarse que la AC raíz es el único componente que no tiene redundancia, ya que, en realidad, este componente no tiene la misma demanda que la AC subordinada que es la encargada de certificar a los ciudadanos y por eso las llavees están en los HSM grandes, los CryptoServer CP5 SE 500. Mientras que la AC raíz solo emite certificados de AC, en este caso a las subordinadas y por lo mismo sus llaves están resguardadas en un HSM de poca capacidad, el CryptpServer CP5 SE12.

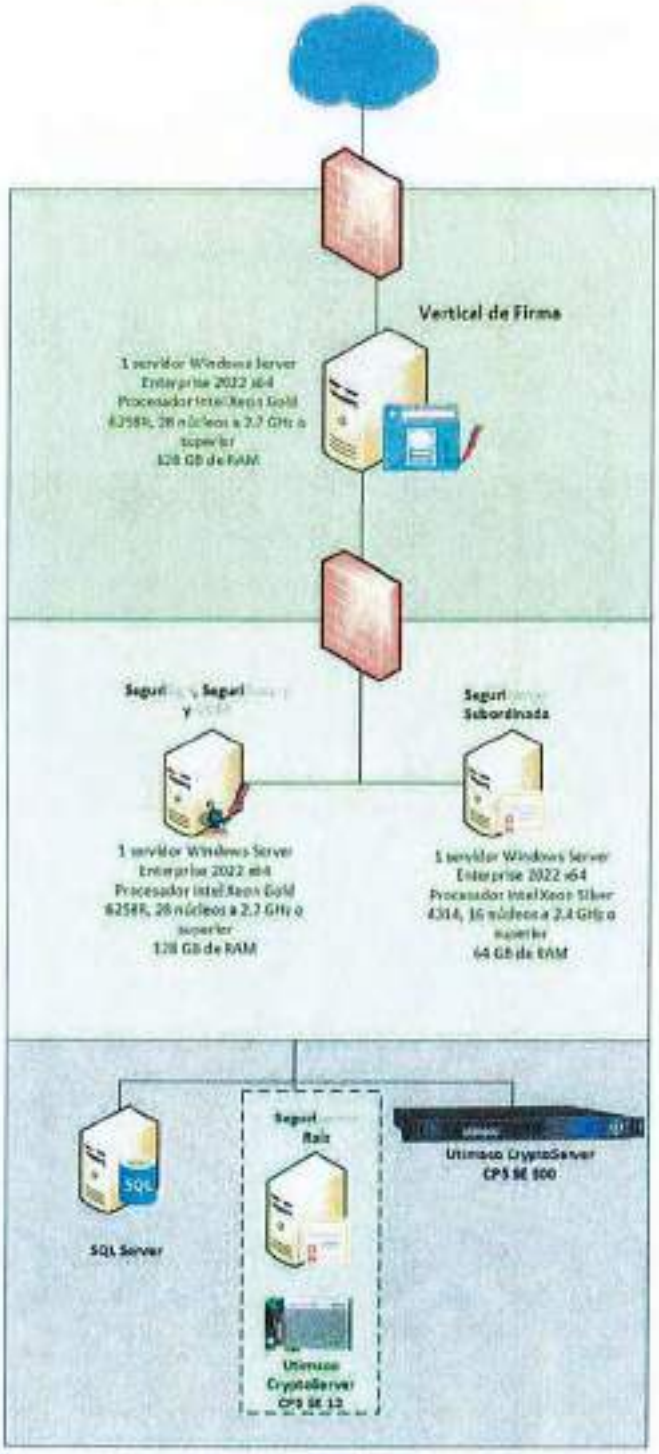
La arquitectura es en tres capas:

- **El Front**, donde se ubica la vertical de firma con sus portales;
- **La capa de aplicación** donde están los servicios de la PKI: SeguriServer (AC subordinada), SeguriNotary (TSA) y SeguriSign (motor de firma); y
- **La capa de datos** donde están las respectivas bases de datos de los componentes y los HSM que resguardan las llaves de las AC: raíz y subordinadas.

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

EMDOC
CONSORCIO

Arquitectura para el ambiente de DRP



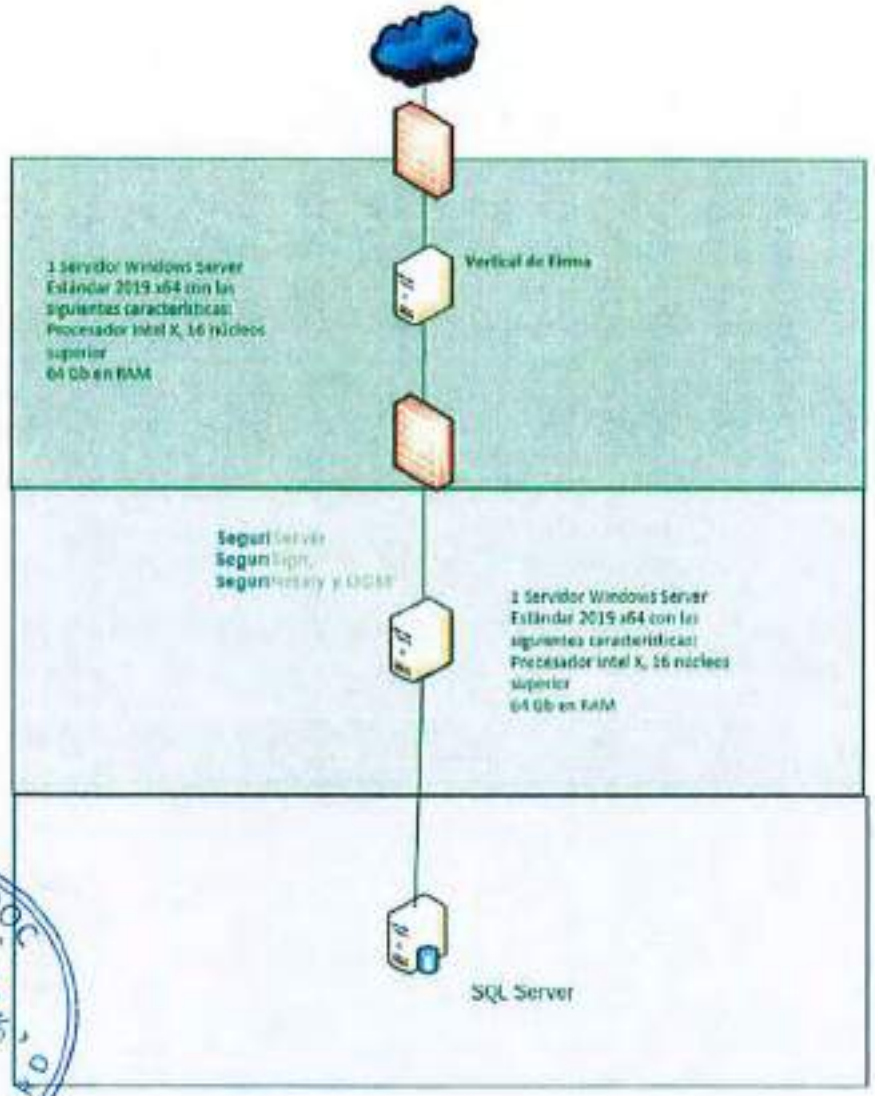
CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

Es la misma configuración que para el ambiente de producción, solamente que el esquema es en disponibilidad simple de los componentes.

Arquitectura para el ambiente de Desarrollo

Misma configuración que para el DRP, sin embargo, aquí no hay HSM y los requisitos del equipo son menores.

Ambiente Desarrollo



1.10 Autoridad Certificadora Raíz

La AC Raíz es el componente más confiable en una PKI, actuando como la fuente principal de verificación y confianza. Esta autoridad es la encargada de emitir certificados digitales a otras autoridades certificadoras (llamadas Autoridades Certificadoras Subordinadas) o a entidades finales u operativas, dependiendo de la estructura de la PKI, esto aplica a lo que estamos planteando que es como dictan las buenas prácticas.

1.10.1 Funcionalidad:

Emisión de Certificados: La AC Raíz emite certificados que verifican la identidad de las Autoridades Certificadoras Subordinadas. Estos certificados sirven como un voto de confianza, asegurando que las subordinadas son entidades confiables.

Creación de Llaves: Genera su propio par de llaves (una pública y una privada) porque es la raíz. La llave privada se utiliza para firmar los certificados de las autoridades subordinadas, mientras que la llave pública se distribuye para verificar esas firmas. Es importante señalar que esta autogeneración de llaves se realiza dentro del módulo criptográfico (HSM), es aquí donde ya encontramos la interoperación entre SeguriServer en su carácter de AC raíz y el HSM. El HSM que empleará la AC raíz es el modelo CryptoServer CP5 SE 12 de Utimaco, ver el respectivo anexo.

Raíz de Confianza: Funciona como el punto más alto de confianza en la PKI. Todos los certificados emitidos pueden ser rastreados hasta este punto, asegurando una cadena de confianza continua.

1.10.2 Beneficios:

Seguridad Mejorada: Al ser la autoridad más alta y centralizada, permite un control estricto de las políticas de seguridad y la emisión de certificados, minimizando la posibilidad de fraude o mal uso de las identidades digitales.

Interoperabilidad: Facilita la comunicación segura entre diferentes sistemas y organizaciones al proporcionar un estándar común de autenticación y cifrado.

Confianza Centralizada: Al ser el punto más alto de confianza, facilita la verificación de identidades y la validación de certificados a lo largo de toda la organización o sistema, sin necesidad de verificar cada conexión de manera individual.

La AC Raíz en una PKI es fundamental para establecer y mantener la integridad, la seguridad y la confianza en las comunicaciones digitales dentro de una organización o entre varias entidades.

Este proyecto considera la implementación de una AC raíz para la JCE.

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

99

1.11 Autoridad Certificadora Subordinada (operativa o ciudadana)

1.11.1 Funcionalidad:

Emisión de Certificados: Las Autoridades Certificadoras Subordinadas son responsables de emitir certificados a entidades finales, como usuarios (ciudadanos) o dispositivos (cédulas de identidad), o a otras AC subordinadas. Estos certificados están firmados digitalmente por la AC subordinada, asegurando así la autenticidad e integridad de la información.

Verificación de Identidades: Antes de emitir un certificado, la AC subordinada verifica la identidad del solicitante, es lo que llamamos el proceso de enrolamiento y que liga la identidad real física) con la identidad electrónica. Este proceso es crucial para mantener la confiabilidad y seguridad de la red.

Gestión de Revocaciones: También manejan las listas de revocación de certificados (CRLs), que son esenciales para mantener actualizado el estatus de los certificados emitidos, identificando aquellos que han sido revocados y no deben ser confiados. Otro mecanismo que es más usado para verificar la revocación es el uso del protocolo OCSP acrónimo Inglés que significa Online Certificate Stauus Protocol, que a diferencia de la CRL con el OCSP se valida en línea, este protocolo lo implementan prácticamente todas las AC, en términos operativos se traduce en un puerto y una dirección IP donde la AC "escucha" peticiones para saber si un certificado está revocado y/o expirado.

1.11.2 Beneficios:

Descentralización del Riesgo: Al distribuir la emisión de certificados a múltiples AC subordinadas, se reduce el riesgo de un punto único de falla que podría comprometer toda la infraestructura de la PKI. En esta propuesta estamos implementando dos AC subordinadas en producción y una en DRP.

Escala y Flexibilidad: Las AC subordinadas permiten a la PKI escalar eficientemente, ya que pueden adaptarse y responder a las necesidades específicas de seguridad de distintos departamentos o sectores dentro de una organización.

Eficiencia en la Gestión: Facilitan la administración de certificados a nivel local (estatal, por ejemplo) o a nivel país, permitiendo una gestión más rápida y cercana a las necesidades específicas de los usuarios finales.

Las Autoridades Certificadoras Subordinadas juegan un papel crítico en la expansión y administración efectiva de una PKI, proporcionando seguridad y confianza en la autenticación y comunicación dentro de redes extensas. Al igual que la AC raíz estas AC subordinadas tendrán resguardadas sus llaves criptográficas en el módulo criptográfico (HSM), a diferencia de la AC raíz las AC subordinadas emplearán el HSM CryptoServer CP5SE 500, esto debido a que la demanda operativa será mucho mayor.

1.12 Portal de Certificación (enrolamiento) empleando las cédulas de identidad

1.12.1 Funcionalidad:

Almacenamiento Seguro de Certificados y Llaves: El chip criptográfico en una tarjeta inteligente permite almacenar de manera segura certificados digitales y llaves criptográficas. Este chip está diseñado para ser resistente a ataques físicos y lógicos, protegiendo la información confidencial.

Autenticación y Firma Digital: Las tarjetas inteligentes con chip criptográfico pueden utilizarse para procesos de autenticación robusta y firma digital de documentos, estos documentos serían el resultado de algún proceso y/o trámite de la JCE que tenga cierto grado de automatización y que requiera firma digital. El chip realiza operaciones criptográficas directamente en la tarjeta, lo que mejora la seguridad al no exponer la llave privada fuera de la tarjeta.

Emisión y Gestión de Certificados: A través del portal de certificación (enrolamiento), los ciudadanos (usuarios) pueden solicitar la emisión o renovación de certificados que se almacenan directamente en el chip de la tarjeta inteligente. Esto puede incluir la generación de pares de llaves donde la llave privada nunca abandona el chip seguro.

1.12.2 Beneficios:

Seguridad Mejorada: La integración de certificados en un chip criptográfico aumenta significativamente la seguridad, dado que las llaves privadas están protegidas contra extracción. Esto minimiza el riesgo de duplicación o uso indebido de las credenciales.

Portabilidad: Las tarjetas inteligentes son dispositivos portátiles que permiten a los usuarios llevar sus credenciales criptográficas de forma segura y utilizarlas en diferentes sistemas, manteniendo la misma identidad digital segura.

Conveniencia y Acceso Controlado: Con las cédulas es posible, por ejemplo, facilitar un acceso controlado a edificios, sistemas de la JCE y otros recursos, combinando seguridad física y lógica en un solo dispositivo.

Cumplimiento de Normativas: Cumplen con estrictas normativas de seguridad y privacidad, lo que las hace adecuadas para industrias reguladas como la financiera, salud y gobierno. Es decir, es muy grande la cantidad de usos que pueden dársele al uso de las cédulas de identidad con chip criptográfico.

Nuestro portal de certificación (enrolamiento) que emite certificados para tarjetas inteligentes con chip criptográfico ofrece una solución robusta y segura para la gestión de identidades y accesos, optimizando tanto la seguridad como la operatividad en diversos entornos.

EMDOC CONSORCIO Santo Domingo, R.D.

1.13 Portal Web de Firma

1.13.1 Funcionalidad:

Firma de Documentos PDF: El portal permite a los usuarios firmar digitalmente documentos en formato PDF, cumpliendo con el estándar PDF Signature (ISO 32000-1). Este estándar garantiza que la firma digital sea válida y reconocida a nivel nacional en este caso, o al menos en el ámbito de la JCE. Sin embargo, decimos a nivel nacional porque las cédulas tendrán validez en todo el país.

Integración con Tarjetas Inteligentes (Smartcards) con chip: Las llaves criptográficas de los usuarios están almacenadas de manera segura en tarjetas inteligentes con chip criptográfico. Cuando un usuario necesita firmar un documento, el portal interactúa con la tarjeta a través de un lector de tarjetas inteligentes para realizar la firma utilizando la llave privada que nunca sale del chip criptográfico.

Autenticación Segura: El acceso al portal requiere autenticación, que puede ser reforzada mediante el uso de la tarjeta inteligente, ya que el portal pide las llaves y la contraseña que protege a la llave privada, proporcionando un nivel adicional de seguridad antes de permitir la firma de documentos.

Gestión de Documentos Firmados: Además de permitir la firma, el portal de firma también ofrece servicios de almacenamiento, seguimiento y verificación de documentos firmados, facilitando la gestión de documentos legales y oficiales.

1.13.2 Beneficios:

Seguridad Avanzada: Al almacenar las llaves criptográficas en tarjetas inteligentes, se protege la identidad y las credenciales del usuario, minimizando el riesgo de robo o abuso de llaves privadas.

Conformidad Legal: Las firmas realizadas cumplen con los estándares legales para firmas digitales, lo que las hace jurídicamente vinculantes y aceptadas en procesos judiciales y administrativos.

Accesibilidad y Conveniencia: Los usuarios pueden firmar documentos desde cualquier lugar donde tengan acceso a Internet y un lector de tarjetas inteligentes, ofreciendo flexibilidad sin comprometer la seguridad.

Integridad del Documento: El uso del estándar PDF Signature asegura que cualquier alteración del documento después de su firma sea detectable, lo que aumenta la confianza en la validez de los documentos firmados.

El portal de firma proporciona una solución eficiente y segura para la firma digital de documentos, aprovechando la tecnología de tarjetas inteligentes para garantizar la seguridad y la autenticidad en general de las transacciones digitales.

1.14 PKI (Infraestructura de Llave Pública)

1.14.1 Componentes de la Infraestructura de Llave Pública (PKI):

SeguriServer (Autoridad Certificadora, AC raíz y subordinada):

- ***Funcionalidad***: Esta AC es responsable de emitir y administrar los certificados digitales almacenados en tarjetas inteligentes con chips criptográficos. SeguriServer genera el par de llaves (pública y privada), donde la llave privada se almacena de forma segura en el chip de la tarjeta inteligente y nunca se expone externamente. Lo anterior a través del portal de certificación (enrolamiento).
- ***Beneficios***: Aumenta la seguridad de las credenciales de identificación, minimizando el riesgo de duplicación o compromiso de las llaves privadas. Facilita el cumplimiento de normativas estrictas de seguridad y privacidad.

SeguriNotary (TSA):

- ***Funcionalidad***: SeguriNotary es una Autoridad de Sellado de Tiempo (TSA) que genera sellos de tiempo (timestamps) para cada firma digital realizada. Esto certifica el momento exacto en que se efectuó la firma, lo cual es crucial para procesos legales y de auditoría.
- ***Beneficios***: Proporciona pruebas irrefutables del momento de la firma, lo que es vital para la validez y la integridad a largo plazo de los documentos firmados digitalmente.

SeguriSign (Motor de firma electrónica):

- ***Funcionalidad***: Este servicio actúa como el núcleo operativo de la plataforma, encargándose de las interacciones entre los usuarios y los componentes tecnológicos. Gestiona la solicitud de sellos de tiempo (timestamps) a SeguriNotary, también se encarga de "preguntar" al servicio de validación en línea de la SeguriServer (OCSP) si un certificado de un usuario está revocado y/o expirado. Almacena en su base de datos los documentos firmados usando el estándar PDF Signature, junto con las respectivas evidencias que acompañan a cada firma: OCSP y sellos de tiempo por cada firma. Además, proporciona APIs y servicios web para que los usuarios puedan firmar documentos directamente desde un portal web o mediante aplicaciones de terceros. Otra gran característica es que SeguriSign puede configurarse para que reconozca a otras AC como de confianza, es decir, lo que se traduce en que pueda reconocer firmas digitales que están empleando certificados que no fueron emitidos por la AC de la JCE.
- ***Beneficios***: Asegura una gestión eficiente de las firmas digitales, permitiendo una fácil integración en diferentes plataformas y aplicaciones mediante sus APIs y Servicios Web. Mejora la accesibilidad y la flexibilidad para los usuarios finales, permitiéndoles firmar y gestionar documentos desde cualquier lugar.

1.14.2 Beneficios Generales de la PKI:

- ***Seguridad Robusta***: La combinación de tarjetas inteligentes, emisión segura de certificados, y sellado de tiempo asegura un alto nivel de seguridad en todo el proceso de firma.
- ***Integridad y Confiabilidad***: La plataforma garantiza que las firmas son válidas, verificables y legalmente vinculantes, gracias a los procesos de validación y certificación que respaldan cada firma.
- ***Cumplimiento de Normativas***: Cumple con normativas internacionales sobre la firma digital y la gestión de identidades digitales, lo que la hace adecuada para su uso en sectores regulados como el financiero, legal y gubernamental.
- **Interoperabilidad y Escalabilidad:** Gracias a las APIs y servicios web, la plataforma puede integrarse fácilmente con otras aplicaciones y sistemas, permitiendo una escalabilidad eficaz conforme crecen las necesidades del negocio.

1.15 Integración de la firma digital con las aplicaciones de la JCE empleando las cédulas de identidad (smartcards con chip)

Antes de describir el proceso general de integración de la firma digital, recordemos que quien orquesta o gestiona las firmas es SeguriSign. A su vez, por cada firma que se ejecuta SeguriSign interopera con Seguriserver para "preguntar" vía el OCSP, si un certificado está revocado o expirado, con SeguriNotary para pedir el sello de tiempo. La realización de la firma del lado del cliente (usuario) desde el navegador de internet se ejecuta por medio de un API y todo el flujo de firma se va tejiendo al invocar de manera propia los servicios web pertinentes.

Entonces ¿Cuáles son los componentes que actúan entre sí para lograr la firma? Estos son:

- **SeguriSign** (motor de firma) como el que orquesta y gestiona la ejecución del proceso de firma, tanto del lado cliente como del lado servidor.
- **SeguriServer**, que mediante su servico de OCSP emite la respuesta hacias SeguriSign de si un certificado (unas llaves criptográficas) no está revocado y/o expirado.
- **SeguriNotary** que emite un sello de tiempo pora cada firma ejecutada, quien se la solicita es SeguriSign.
- **Portal Web** o aplicación que implementa o integra la firma digital, este sería el cliente, para el caso de la solución presentada quién hace esto es nuestro portal de firma, es decir, es un ejemplo de cómo implementar firma desde un portal web.
- Desde luego los **servicios web de SeguriSign**.

- **API criptográfico** que se usa en el browser para gestionar la interacción entre la aplicación web y el lector de tarjetas para acceder a las llaves contenidas en la cédula de identidad, es decir, la smartcard.

Ahora procedemos a explicar el proceso de cómo sucede la integración de la firma digital y una aplicación por ejemplo de la JCE con los componentes mencionados, que forman parte de la PKI.

1.15.1 Proceso de Integración de la Firma Digital con Llaves en Smartcard:

Nota: cuando se lea "el cliente", se debe entender la aplicación de la JCE.

1. Inicialización del Proceso de Firma:

- ***Desde el cliente***: La aplicación cliente inicia el proceso de firma interactuando con un servicio web de SeguriSign. Esta solicitud inicial especifica quiénes firmarán, qué documento se va a firmar y el estándar de firma digital a aplicar.
- ***Respuesta de SeguriSign***: SeguriSign asigna un identificador único al proceso de firma y guarda los detalles pertinentes. Este identificador se usará para gestionar todo el proceso de firma.

2. Solicitud de Hash del Documento:

- ***El cliente solicita el hash***: La aplicación cliente, mediante la invocación a otro servicio web, solicita a SeguriSign el hash del documento que se va a firmar. Este paso requiere autenticación para asegurarse de que sólo los participantes autorizados obtengan el hash. En este caso los ciudadanos enrolados.
- ***Respuesta con el hash***: SeguriSign proporciona el hash del documento, que es esencial para la firma digital.

3. Firma del Hash con la Llave Privada:

- ***El API criptográfico*** *interactúa con la cédula de identidad (smartcard)*: El API criptográfico gestiona la interacción con la cédula de identidad (smartcard) para acceder a la llave privada del usuario, que está protegida y nunca sale del chip criptográfico. El usuario proporciona la contraseña para desbloquear su llave privada, y el API utiliza esta llave para firmar el hash del documento.
- ***Proceso seguro en la smartcard***: La operación de firma se realiza dentro del entorno seguro del chip criptográfico, asegurando que la llave privada no sea expuesta ni comprometida.

4. Envío de la Firma Digital a SeguriSign:

- ***El cliente envía la firma***: Tras obtener la firma digital, el cliente usa un servicio web para enviar esta firma a SeguriSign.

CONSORCIO EMDOC Santo Domingo, R.D.

- ***Recopilación de firmas***: SeguriSign recopila y asocia cada firma recibida con el proceso de firma correspondiente, es decir, va recopilando las firmas de cada uno de los firmantes, si es que son 2 o más, o también si solo es uno, aquí podemos suponer que son dos o más.

Nota: Los pasos 2, 3 y 4 se repetirán por cada usuario que participe en el flujo de firma lanzado en el paso 1.

5. Finalización y Notificación:

- ***Cierre del proceso***: Cuando todos los firmantes han completado sus firmas, SeguriSign finaliza el proceso de firma.
- ***Notificaciones a los participantes***: SeguriSign notifica a todos los firmantes que el documento ha sido completamente firmado y que el proceso ha concluido con éxito. Con lo cual pueden descargar el documento ya firmado por todos, se invoca otro servicio web para esto.

Beneficios Clave de Usar Smartcards y el API de JavaScript:

- ***Protección avanzada de llaves privadas***: Las llaves almacenadas en chips criptográficos de smartcards ofrecen un nivel superior de seguridad contra robos o exposición.
- ***Integridad y Autenticidad***: La firma realizada en el chip garantiza que el documento firmado no pueda ser alterado sin detectarse, proporcionando una robusta evidencia de integridad y autenticidad.
- ***Conformidad y Validez Legal***: Las firmas realizadas cumplen con normativas de seguridad y autenticación digital, haciéndolas legalmente vinculantes.
- ***Accesibilidad y Flexibilidad***: Los servicios web y el API de JavaScript permiten una integración fácil y segura en cualquier aplicación, proporcionando a los usuarios la capacidad de firmar documentos de manera eficiente y segura desde cualquier lugar.

Este enfoque no solo maximiza la seguridad durante el proceso de firma digital, sino que también asegura que la solución sea escalable, accesible y cumpla con los más altos estándares de conformidad legal y seguridad informática.

1.16 Mantenimiento del licenciamiento de la PKI

Se incluye el mantenimiento del licenciamiento de los componentes de la solución para dar el servicio cubriendo los siguientes elementos:

- Software SeguriServer
- Software SeguriNotary

- Software SeguriSign
- Vertical de Firma
- Software Portal de Certificación (enrolamiento)
- API criptográfica con soporte a PKCS#11

Se entiende por mantenimiento la actualización a los productos de ***SeguriData*** (SeguriServer, SeguriNotary, SeguriSign, Vertical de Firma, Portal de Certificación, API con soporte a PKCS#11, en los ambientes de producción, DRP y desarrollo que la JCE tendrá, a fin de conservarlos en condiciones óptimas de funcionamiento, de acuerdo a sus propias especificaciones técnicas.

Upgrades

Son adecuaciones mayores que consisten en nuevas funcionalidades de los productos y tienen las siguientes características:

- Actualización para cumplir con los estándares de seguridad.
- Incorporación de nuevos módulos y protocolos de comunicación.
- Adecuaciones para cubrir con reglamentos y leyes Nacionales e Internacionales.
- Soporte a nuevos sistemas operativos y nuevas versiones de sistemas operativos ya existentes.

Las nuevas versiones serán enviadas a la JCE, en un plazo no mayor de 30 días hábiles, después de su liberación formal.

Updates

Son adecuaciones menores y consisten en el arreglo de problemas detectados en versiones anteriores o bien en modificaciones a la interfaz gráfica. Los updates serán enviados a la JCE, en plazo no mayor de 15 días hábiles, después de su liberación formal.

1.17 Servicios de soporte técnico 7x24 de los productos y componentes

La vigencia de la póliza de soporte técnico remoto será 7x24, durante la vigencia del contrato, con las siguientes características:

- 160 (ciento sesenta) horas anuales vía remota, correo electrónico o telefónico.
- Horario de atención de 24 (veinticuatro) horas, los 7 (siete) días de la semana, los 365 (trescientos sesenta y cinco) días del año.
- Se incluyen los servicios de soporte a los productos de software: SeguriServer, SeguriNotary, SeguriSign, Vertical de Firma, Portal de Certificación, API con soporte a PKCS#11, de acuerdo con lo siguiente, descrito de manera enunciativa mas no limitativa:

CONSORCIO EMDOC Santo Domingo, R.D.

- Brinda asesoría técnica y asistencia sobre el funcionamiento, operación y administración.
- Proporciona los parches a la JCE en caso de alguna falla del producto.
- Atención y resolución de incidencias presentadas en el software: SeguriServer, SeguriNotary, SeguriSign, Vertical de Firma, Portal de Certificación, API con soporte a PKCS#11, conforme al acuerdo de nivel de servicios de soporte técnico del pliego de requisitos, mismo que se señala a continuación:

1.17.1 Soporte Técnico del HSM

La propuesta incluye una Póliza de Mantenimiento Premium para el equipo criptográfico marca Utimaco, directamente del fabricante, además del respaldo para brindar soporte de primer nivel

Las características de la póliza de soporte de mantenimiento Premium incluye:

- Acceso 24x7 al equipo de soporte Helpdesk vía portal web, teléfono y email
- Respuesta inicial en menos de 2 horas
- Reemplazo de hardware en caso de ser necesario.
- Software, firmware y documento de actualizaciones

1.18 Duración del Servicio

Por tratarse de un documento de seguridad y para mantener la homogeneidad o igualdad, tanto en la impresión, como en las características técnicas que habrán de emplearse en la elaboración de la nueva Cédula de Identidad y Electoral y la Cédula de Identidad, el contrato para la producción será por el período de vigencia de la nueva Cédula de Identidad y Electoral y Cédula de Identidad, diez (10) años, por lo que cada Oferente propondrá su mejor programa de producción o entrega y la Junta Central Electoral evaluará en función de su máximo interés.

1.19 Lugar y Programa de Suministros

Los pedidos se librarán en el lugar designado por la JCE dentro del ámbito territorial de la República Dominicana y conforme al cronograma de entrega que se establezca. En caso de no especificarse, se entenderá que el lugar de entrega será la sede principal de la Junta Central Electoral.

1.20 Entregables del Proyecto

No.	Entregables	Descripción
		Licenciamiento perpetuo para:

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo R.D.

1	**Licenciamiento perpetuo**	• Software SeguriServer:3 instancias x procesador y 1 instancia servidora • Software SeguriNotary:3 instancias x procesador y 1 instancia servidora • Software SeguriSign:3 instancias x procesador y 1 instancia servidora • Software Vertical de Firma:3 instancias por procesador y 1 instancia servidora • Software Portal de Certificación:3 instancias por procesador y 1 instancia servidora • API con soporte a PKCS#11
2	**Póliza de soporte técnico remoto 7x24 al software de la PKI**	Póliza de soporte técnico remoto 7x24 con vigencia por la duración del contrato y ampara a todos los componentes de software de la PKI.
3	**Póliza de mantenimiento al software de la PKI**	Póliza de mantenimiento para tener las versiones más recientes y en óptimas condiciones de los componentes de software de la PKI, durante la vigencia del contrato.
4	**Módulos criptográficos**	3 módulos criptográficos con las especificaciones del apartado 5.1.6 Descripción técnica de Módulo CryptoServer CR5 SE 500 de Utimaco. 2 módulos criptográficos con las especificaciones del apartado 5.1.7 Descripción técnica de Módulo CryptoServer CR5 SE 12 de Utimaco. 5 pólizas de mantenimiento Premium para los 5 equipos criptográficos durante la vigencia de la contratación.
5	**Instalación y configuración de la PKI de la JCE**	• Orden de Servicio firmada por el responsable del proyecto, con la descripción de las actividades realizadas en el servicio de instalación y configuración. • Memoria técnica con el detalle de la instalación y configuración de los

CONSORCIO EMDOC Santo Domingo, RD

		componentes de la PKI, tanto los de software como los módulos criptográficos para los tres ambientes.
6	**Acompañamiento y Asistencia técnica a la Normatividad de la Autoridad Certificadora.**	• Script de creación de llaves de la Autoridad Certificadora de la JCE. • Plantillas para la generación de las Políticas de Certificación y Declaración de Prácticas de Certificación (CP y CPS según RFC 3647).
7	**Capacitación (Transferencia de conocimientos)**	• Autorización firmada por el responsable del proyecto, con la descripción de las actividades realizadas en el servicio. • Material de capacitación digital • Lista de asistencia del personal capacitado
8	**Acompañamiento y Asistencia técnica a la Integración.**	• Orden de Servicio firmada por el responsable del proyecto, con la descripción de las actividades realizadas en el servicio.

1.21 Anexos a Solución PKI

1.21.1 Descripción técnica funcional de productos PKI

Descripción técnica autoridad certificadora (SeguriServer)

Software encargado de facilitar la administración del ciclo de vida de los certificados digitales, desde la emisión hasta la revocación de los certificados, para facilidad de operación SeguriServer cuenta con los siguientes componentes:

A. MÓDULO DE AUTORIDAD CERTIFICADORA

- Soporta su instalación en equipos con sistema operativo Microsoft Windows Server 2019 64 bits o superior.
- Cuenta con una consola gráfica de configuración para facilitar al administrador su operación y configuración.
- Puede establecer el puerto TCP de operación del servicio para comunicación de aplicaciones de acuerdo a las definiciones del contratante.
- Soporta los servidores de Base de Datos siguientes, para almacenamiento y administración de la información:
  - Microsoft SQL Server 2012 o superior
  - Oracle
- Cuenta con soporte para integración con el protocolo SMTP para comunicaciones con servidores de Correo Electrónico, para el envío de notificaciones de certificación.
- Permite la personalización del mensaje de notificaciones de correo electrónico de acuerdo a las necesidades de la institución.
- Soporta la emisión y administración ilimitada de Certificados Digitales.
- Soporta al menos 2 formatos de números de serie para los certificados digitales, secuenciales o extendidos.
- Cuenta con un módulo de auditoría de operaciones de la Autoridad Certificadora, este funciona a través de la emisión de recibos criptográficos (bajo el estándar RFC3161), garantizando la integridad de las operaciones y de la base de datos para todo el ciclo de vida de los certificados:
  - Emisión
  - Verificación de estado
  - Revocación
- Las transacciones entre la autoridad registradora, los servicios de validación y la autoridad certificadora están cifradas electrónicamente de

acuerdo a los algoritmos utilizados LFFEA para la generación de certificados en caso de requerirse.

- Soporta varios servicios de Autoridad Certificadora en el mismo equipo, cada servicio es independiente y puede configurarse individualmente.
- Soporta al menos 3 niveles de profundidad para la subordinación de autoridades.
- Proporciona escalabilidad en la infraestructura en cuanto a la capacidad de atención de múltiples transacciones simultáneas.
- Soporta su configuración en ambientes distribuidos como; clústeres y granjas, garantizando balanceo de cargas.
- Soporta ambientes en alta disponibilidad.
- Permite definir extensiones para los certificados digitales, tales como:

Netscape Certificate Type	TLS Web Client Authentication
SSL Client Authentication	Code Signing
SSL Server Authentication	Secure e-mail
S/MIME (Client)	Time Stamping
Object Signing	OCSP Signing
SSL CA	Microsoft Strong Encryption
S/MIME CA	Encrypting File System
Object Signing CA	Microsoft Smart Card Logon
Key Usage	Netscape Strong Encryption
Digital Signatura	Subject Alternative Names
Non repudiation	Issuer Alternative Names
Key Encipherment	Certificate Policies
Data Encipherment	URL
Key Agreement	Text
Cert Signing	CRL Distribution Point (CDP)
CRL Signing	URL
Encipher Only	Authority Info Access (AIA)
Decipher Only	URL
Enhanced Key Usage	LDAP / http Certificate address

- Soporta su implementación en ambientes virtualizados.
- Puede genera certificados cumpliendo con el RFC5280.
- Soporta la generación de llaves criptográficas RSA de 2048 bits recomendadas para usuarios o servicios.
- Soporta la generación de llaves criptográficas RSA de 4096 bits recomendadas para Autoridades Certificadoras
- Soporta la generación de llaves criptográficas ECC para emplearse con ECDSA, usando las curvas estándar P-224, P-256, P-384 y P-521, recomendadas por NIST.

- Permite emitir extensiones en certificados X.509 para hacer posible la conversión a certificados EDIFACT. Los certificados EDIFACT cumplen con las Guías de implantación mexicanas para seguridad EDIFACT normada por AMECE en los documentos:
  - Servicio de Autenticación de Origen, Integridad y No Repudiación de Origen.
  - Llave de Seguridad y Manejo de Certificado (KEYMAN).
  - Documentos basados en el ISO 9735-5 e ISO 9735-9 respectivamente
- Cuenta con un módulo de conversión de archivos PKCS#12.
- Registra y mantiene bitácoras que permiten el monitoreo de los servicios.
- Soporta en sus diferentes operaciones al menos los siguientes estándares o algoritmos criptográficos:

X.509 V1 y V3 - IETF RFC 3280	PKCS#5
FIPS 140 V2 N3.	PKCS#10
PKCS	PKCS#11
PKCS#1(RSA)	PKCS#12
LDAP	PKCS#5
CRL (RFC 3280, X.509)	SHA256
OCSP (RFC 2560)	SHA512

- Integra y ofrece la funcionalidad para verificar el estado de revocación de un certificado digital, ofreciendo:
- Módulo servidor OCSP para la verificación en línea del estado de revocación de un certificado digital.
- Módulo para la generación automática periódica de la Lista de Certificados Revocados (CRL).
- Garantiza una disponibilidad del 99% en el servicio de consulta del estatus de los certificados digitales a través de OCSP o CRL en condiciones normales.
- Considera un tiempo de indisponibilidad máximo de 4 horas en caso de desastre para los servicios de revocación y un tiempo máximo de 2 horas para los servicios de consulta de estatus (CRL u OCSP).

B. MÓDULO DE LLAMADAS EXTERNAS

- La solución cuenta con un módulo que permite agregar funcionalidad mediante llamadas a una librería dinámica que exporte funciones de acuerdo a una interfaz especifica.
- El uso de la librería especifica se puede configurar en la interfaz de configuración de la Autoridad Certificadora.
- Las llamadas podrán realizarse al momento de emitir, revocar un certificado digital o en ambos casos.

C. MÓDULO DE HARWARE CRIPTOGRÁFICO

- Compatibilidad para interactuar con dispositivos de hardware criptográficos que cuenten con la certificación FIPS-140-2 Nivel 3 en modalidad de conexión USB, PCI o red.
- Considerando las características de los módulos de hardware criptográfico para el resguardo de las llaves de la Autoridad Certificadora, especificadas en la sección de requerimientos mínimos y funcionales del Anexo Técnico al cual atiende esta propuesta técnica.
- La comunicación a los dispositivos criptográficos es a través del protocolo PKCS#11.
- Cuenta con los mecanismos necesarios para soportar un esquema de custodios para el acceso al dispositivo.

D. MÓDULO DE ADMINISTRACIÓN

- Cuenta con una consola de administración que ofrece la siguiente funcionalidad:
  - Administración de Autoridades Certificadoras subordinadas
  - Administración de Autoridades Registradoras
  - Autorización de emisión de Certificados Digitales.
  - Solicitud de revocación de Certificados Digitales.
  - Solicitud de CRL's.
  - Búsqueda de Certificados Digitales.
  - Soporta diferentes modelos de autenticación (login) del usuario soportando autenticación por software y a través de dispositivos criptográficos.
  - Al momento de aprobar la emisión de un Certificado Digital permite especificar las fechas (día) de inicio y expiración usando un calendario.

E. MÓDULO DE AUTORIDAD REGISTRADORA

- Soporta su instalación en un equipo con sistema operativo Microsoft Windows 10, Microsoft Windows Server 2016 64 bits o superior.
- Cuenta con una consola a través de la cual se pueden ejecutar las siguientes operaciones:
  - Autorización de emisión de Certificados Digitales.
  - Solicitud de revocación de Certificados Digitales.
  - Solicitud de CRL's.
  - Búsqueda de Certificados Digitales.
  - Búsqueda de Requerimientos de Certificación (Generación Web).

- Soporta la autenticación al módulo mediante certificados digitales.
- Al momento de aprobar la emisión de un Certificado Digital permite especificar las fechas (día) de inicio y expiración usando un calendario.

F. INTEFAZ WEB

- Cuenta con una aplicación de tipo Web donde se ofrecen servicios a los usuarios, estos servicios son:
  - Generación de llaves y Requerimiento de Certificación con soporte de múltiples CSP (Cryptographic Service Provider), para resguardar la llave en dispositivos criptográficos vía Web, además de su envío a la Autoridad Certificadora.
  - La generación de llaves no depende de tecnologías propietarias, ejemplo, ActiveX o Applets, es decir, es independiente del navegador web, soporta al menos equipos Windows 7, 8, 10 y Mac (Yosemite, Catalina).
  - Soporta clientes con sistemas operativos Microsoft Windows XP, Microsoft Vista, Microsoft Windows 7, Microsoft Windows 8, Microsoft Windows 10 Microsoft Windows Server 64 bits o superior.
  - Envío a la Autoridad Certificadora del Requerimiento de Certificación a partir de archivo en formato PKCS#10.
  - Instalación de Certificados Digitales.
  - Consulta de Certificados Digitales y opción a descarga de los mismos.
  - Solicitud y descarga de una CRL.
  - Solicitud y descarga del Certificado Digital de Autoridad Certificadora.
  - Revocación de Certificados Digitales a partir de una clave de revocación.
  - Revocación de Certificados Digitales a partir de su autenticación al servidor Web utilizando SSL con autenticación de usuarios.
  - La aplicación Web permite la modificación de la interface gráfica de acuerdo a la imagen de la institución.
  - La aplicación de generación de llaves e instalación de certificados digitales soporta el uso de tarjetas inteligentes o dispositivos criptográficos.
  - La aplicación Web soporta su implementación en sistemas operativos tanto Windows como UNIX.
  - Funcionamiento del portal bajo protocolo seguro de comunicación HTTPS.

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

G. INTERFAZ DE DESARROLLO

- Cuenta con herramientas y servicios que permiten su integración a aplicaciones propietarias o de terceros, que soportan los sistemas operativos:
  - Microsoft Windows 10, Microsoft Windows Server 2016 64 bits of superior.
  - UNIX (Solaris, Red Hat, AIX)
- Cuenta con API's con base en lenguajes de programación "C" y "Java", que provean las siguientes funcionalidades:
  - Emisión de Certificados Digitales.
  - Consulta de Certificados Digitales.
  - Revocación de Certificados Digitales.
  - Consulta de CRL's.

H. MÓDULO OCSP RESPONDER

- Trabaja bajo el protocolo OCSP (RFC 2560).
- Soporta su instalación en un equipo con sistema operativo Microsoft Windows Server 2012 o superior.
- Permite configurar los tres esquemas de validación definidos por el RFC 2560:
  - AC que emitió el certificado en cuestión (Issuer CA).
  - Un respondedor confiable para el solicitante (Trusted Responder).
  - Un respondedor autorizado por la AC (Authorized Responder)
- Responde a paquetes con múltiples certificados (emitidos por la misma autoridad).
- Cuenta con API's que permiten generar las peticiones hacia el servicio para la validación de estatus.
- Cuenta con un cliente gráfico que permita realizar consultas por certificados específicos.
- Permite su operación y configuración en sistemas distribuidos como clústeres o granjas para garantizar balanceo de cargas o alta disponibilidad.
- Soporta su implementación en ambientes virtualizados.
- Cuenta con una consola de configuración donde se establecen:
  - Autoridades Certificadoras de Confianza y su configuración.
  - Par de llaves para operación del servicio.

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

- Permite establecer el puerto TCP de operación del servicio para comunicación de aplicaciones de acuerdo a las definiciones del cliente
- Permite la administración del servicio, el poder iniciarlo y detenerlo.
- Permite registrar servicios OCSP de cualquier Autoridad Certificadora.
- Permite su configuración como OCSP intermediario que sirve como punto único de contacto para facilitar la integración de los componentes de PKI en arquitecturas de más de una Autoridad Certificadora.
-

I. CONSIDERACIONES GENERALES

- Los componentes de la autoridad certificadora son modulares y permiten crear entornos distribuidos para cualquier tipo de configuración.
- Las características de sus componentes permiten configurar entornos de balanceo de carga en modalidad activo-activo.
- La modularidad de la aplicación permite establecer políticas restrictivas entre servidores.
- La fecha y hora de emisión d ellos certificados son obtenidos directamente de los equipos en donde se ejecutan las consolas de agente o administrador.
- Tiene la capacidad de crear diversas Autoridades Certificadoras cada una con parámetros de operación independientes.
- Tiene la capacidad de crear una o más Entidades Registradoras por Autoridad Certificadora.
- Tiene la definición paramétrica de perfiles para la ejecución de funciones de administración, agentes registradores y agentes certificadores.
- Tiene la capacidad para definir de forma paramétrica la asignación de extensiones a ser aplicados a certificados digitales.
- Puede generar correos electrónicos paramétricos para notificación a solicitantes de certificados digitales.
- Puede generar correos electrónicos paramétricos para notificación a administradores de la Autoridad Certificadora y Registradora.
- Tiene definición paramétrica de reglas para publicación de certificados digitales.
- Da cumplimiento a lineamientos establecidos por entidades reguladoras, tales como: SAT, SE, Banxico.

J. LA GENERACIÓN DE CERTIFCADOS DIGITALES X.509

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

- Soporta los siguientes estándares o algoritmos criptográficos en su operación:
  - X.509 – (RFC 3280)
  - En las siguientes versiones del certificado X.509 V1, V2 y V3.

1. Versión	V3
2. Serial Number	Número secuencial del Certificado Digital emitido por la AC.
3. Signature Algorithm	SHA256withRSAEncryption SHA1withRSAEncryption
4. Issuer Distinguished Name	CN=AC DNIE XXX OU=SEGOB O= DGRNPIP C=MX S=DF
5. Validity	Not Before: Jul 1 16:04:02 2008 GMT Not After: Dec 31 16:04:02 2010 GMT
6. Subject	CN=APELLIDO1 APELLIDO2, NOMBRE(S) G=NOMBRE SN= FECHA DE NACIMIENTO C= MX
7. Subject Public Key Info	Algoritmo: RSA Encryption Longitud clave: 1024 bits

- Anexo V2

1. issuerUniqueIdentifier	RFC
2. subjectUniqueIdentifier	CURP

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

1.21.2 Descripción técnica de Autoridad Emisora de Estampas de Tiempo (TSA - SeguriNotary)

Software encargado de emitir acuses de recibo permitiendo demostrar la existencia de la información en un tiempo determinado.

A. MÓDULO DE ADMINITRACIÓN DE ESTAMPILLAS ELECTRÓNICAS

- Plataforma sistema operativo Microsoft Windows Server 2016 64 bits o superior.
- Módulo de consola gráfica de configuración para facilitar al administrador su operación y configuración.
- Operación y comunicación del servicio basada en TCP.
- Operación con base de datos:
  - Microsoft SQL Server 2016 o superior
  - Oracle
  - IBM DB2
- Soporta múltiples servicios de Autoridad de Estampillas de Tiempo independientes en el mismo equipo.
- Infraestructura escalable soportando múltiples transacciones simultáneas.
- Garantiza la integridad de los sellos de tiempo, es decir, tiene mecanismos criptográficos que permiten validar que el sello no ha sido alterado.
- Garantiza que la información que resguarda los sellos de tiempo, incluidas los mecanismos criptográficos de validación, pueda ser auditada para determinar su integridad, es decir, verifica que no se produzca alguna modificación en la información, de tal manera que puede reportarse en una auditoría todos aquellos registros que han sufrido alteración.
- Genera Estampillas de Tiempo de Acuerdo al protocolo TSP (RFC 3161).
- Cuando se cuenta con un PKCS#7, elservicio puede entregar como resultado un CAdES-A que tiene insertado un sello de tiempo de archivado (ATSv3) según el estándar ETSI TS 101 733 v2.2.1 sobre documentos CAdES-BES/EPES/T/XLong/XL T1/XL T2/A.
- El cliente mencionado en el numeral anterior también permite procesar un documento XML-Sig como entrada y la salida en este caso es un sello de archivado para XAdES según el estándar ETSI TS 103 171 v2.1.1, para ser embebidas en archivos XAdES-LT.
- Módulo de auditoría automático para operaciones de Autoridad de Estampillas de Tiempo, garantizando la integridad de los recibos emitidos mediante el cifrado electrónico de los registros de base de datos.
- Soporta su implementación en ambientes virtualizados.
- Soporta operación en alta disponibilidad en arquitectura tipo Clúster.

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

- Servicios web tipo REST con soporte mandatorio a TLSv1.2.
- Comunicación de servicios web bajo protocolo seguro de comunicación HTTPS.
- El sello digital de tiempo está compuesto por los siguientes elementos básicos:
    - Datos sobre la identidad de la autoridad emisora (identidad jurídica, clave pública a utilizar en la verificación del sello, numero de bits de la clave, el algoritmo de cifrado digital y la función hash utilizada).
    - Tipo de solicitud cursada (si es un valor hash o un documento).
    - Parámetros del secuenciador (valor hash de la transacción consecutiva).
    - Fechas utilizadas en formato Internet date / time UTC (AAMMDDhhmmss).
    - Evidencias criptográficas de todo lo anterior con la clave pública y esquema de cifrado digital.
- Estándares o algoritmos criptográficos soportados:

RSA	SHA256
PKCS	SHA384
X.509 - IETF RFC 3280	SHA512
PKCS#5	MD5
SHA1	TSP – IETF RFC 3161
SHA224	

B. MÓDULO DE ADMINISTRACIÓN

- Plataforma con sistema operativo Microsoft Windows Server 2016 o superior. Operaciones soportadas para las pistas de auditoría sobre transacciones registradas:
    - Consulta.
    - Extracción de información.
    - Generación de reportes.

C. INTERFAZ DE DESARROLLO

- Plataforma con sistema operativo:
    - Microsoft Windows Server 2019 64 bits ó superior
    - UNIX (Solaris, Red Hat, AIX, Suse)
- Herramientas y servicios para desarrolladores para integración de funcionalidad en aplicaciones propietarias o de terceros.
- API's basados en lenguajes de programación "C", y "Java", proporcionando funciones de:

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, RD

- Solicitud de generación de estampillas de tiempo
- Autenticación de estampillas de tiempo.

1.21.3 Descripción técnica de Motor de Firma Electrónica (SeguriSign)

Software de firma o de criptografía asimétrica SeguriSign que provee múltiples servicios que permiten a una aplicación de terceros realizar el registro, autentificación y generación de evidencias criptográficas para conformar documentos cifrados electrónicamente, auto auditables y con resguardo de evidencias criptográficas que incluyan sellos digitales de tiempo.

A. MÓDULO DE ADMINISTRACIÓN Y AUTENTICACIÓN DE EVIDENCIAS CRIPTOGRÁFICAS

- Soporta su instalación en equipos con sistema operativo Microsoft Windows Server 2019 64 bits o superior.
- Esta bajo la categoría software como servicio (SaaS, del inglés Software as Service).
- Proporciona escalabilidad en la infraestructura en cuanto a la capacidad de atención de múltiples transacciones simultáneas.
- Soporta su instalación y operación en sistemas distribuidos como Clústeres y Granjas para garantizar el balanceo de cargas.
- Soporta su implementación en ambientes de alta disponibilidad.
- Soporta su implementación en ambientes virtualizados.
- Soporta el uso de varios servicios de autenticación de evidencias criptográficas en el mismo equipo, cada servicio deberá administrarse de manera independiente.
- Cuenta con una consola gráfica de configuración para facilitar al administrador su operación.
- Permite establecer el puerto TCP de operación del servicio, para comunicación de aplicaciones de acuerdo a las definiciones del cliente.
- Soporta los siguientes servidores de Base de Datos para almacenamiento y administración de la información.
  - Microsoft SQL Server 2016 o superior
  - Oracle
- Permite la verificación del estado de revocación de un Certificado Digital, conectándose a un Servidor OCSP y a través de una lista CRL.
- Permite la integración a una Autoridad de Estampillas de Tiempo para la generación de las mismas (bajo el estándar RFC 3161).
- Permite la operación con al menos 2 Autoridades Certificadoras de Confianza.

- Permite la interoperabilidad con los módulos para la solicitud de cadenas de certificados y validación del estatus de revocación.
- Permite la solicitud y almacenamiento de constancias de la NOM151 para la conservación de mensajes de datos.
- Soporta al menos los siguientes estándares o algoritmos criptográficos para su operación:

X.509 – (RFC 3280)	ECDSA/P-256
PKCS # 1 (RFC8017).	ECDSA/P-384
PKCS#5 (RFC2898)	ECDSA/P-521
CMS (RFC 5652)	OCSP (RFC 2560)
PKCS#12 (RFC7992)	CRL (RFC 3280)
PKCS#15	TSP (RFC 3161)
RSA/SHA1	PDF Signature ISO 32000-1.
RSA/SHA256	LDAP
RSA/SHA512	
ECDSA/P-224	

- Puede almacenar las evidencias criptográficas con contenido y sin contenido de los documentos y transacciones.
- El archivo cifrado electrónicamente es independiente del equipo de cómputo dónde se realiza la transacción de cifrado o del sistema operativo del cual se intercambia el documento.
- Soporta el formato CAdES, así como el formato PAdES.
- Soporta la comprobación de las evidencias criptográficas a través de cualquier visor PDF con soporte para el estándar ISO 32000-1.
- Soporta el uso de llaves criptográficas en formato PKCS#12, al igual que en formato .cer y .key.
- Ofrece los componentes tipo API y Servicios Web que permiten consumir en aplicaciones de terceros la funcionalidad para validar los certificados y generar estampillas de tiempo con la finalidad de conformar documentos encriptados electrónicamente bajo el estándar PDF Signature.
- La plataforma puede integrarse a cualquier sistema que pueda utilizar o consumir Servicios Web.

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

- Los servicios para PDF Signature, pueden ejecutarse lo mismo desde una computadora de escritorio, así como desde un teléfono inteligente o tableta con sistema operativo iOS o Android en sus versiones más recientes.
- Cuenta con un Portal Web disponible para generar múltiples flujos que permita obtener las evidencias criptográficas de los firmantes de un documento electrónico en particular (firmantes, destinatarios, fecha de expiración de proceso de firma e incluir notas).
- El Portal Web cuenta con la capacidad para poder utilizar distintos dispositivos criptográficos que resguarden la llave privada del usuario.
- El Portal Web cuenta con un control de acceso a través de autenticación de certificado digital.
- Funcionamiento del portal bajo protocolo seguro de comunicación HTTPS.
- El Portal web de gestión del ciclo de vida de los certificados digitales (emisión y revocación) que se emitirán a la ciudadania y que se podrán almacenar en las cédulas de identidad, como una solución web con granuralidad en los permisos o dicho de otro modo, control de acceso. Asi como poder realizar consultas o reportes de los certificados. 1
- El portal web de la gestión del ciclo de vida de los certificados, se brinda para el personal de la JCE.
- Para ingresar al portal web cada usuario debe tener un certificado de autenticación.

B. VALIDACIONES DE EVIDENCIAS CRIPTOGRÁFICAS BAJO EL ESTÁNDA PDF SIGNATURE

- Al abrir un archivo con evidencias criptográficas a través de un visor PDF soporta el estándar ISO 32000-1, se puede comprobar lo siguiente:
  - Que se cumpla con la integridad de la información cifrada.
  - La validez de los certificados implicados.
  - Que el certificado de firma ha sido emitido por la Autoridad Certificadora aceptada como de confianza.
  - Verificar de forma automática la integridad y autenticidad del documento sin necesidad de abrirlo con un visor PDF.
- Un documento firmado bajo el estándar PDF Signature, contiene las siguientes evidencias criptográficas:
  - Respuesta OCSP del certificado del firmante.
  - Sello digital de tiempo.
  - Certificado del firmante.
  - Certificado de la Autoridad Certificadora emisora del firmante.

CONSORCIO EMDOC Santo Domingo, R.D

- Certificado de la Autoridad Emisora de Estampillas de Tiempo que emite el sello digital de tiempo.
- CMS (del inglés Cryptographic Message Syntax) embebido en el PDF Signature

- Soporte a Long Term Validation (LTV) acorde a las condiciones de operación.

C. COMPONENTES CLIENTE

- Componente de firma en cliente para navegadores web.
  - No depende de tecnologías propietarias como Applet o ActiveX.
  - No requiere instalarse nada en el equipo cliente.
  - Soporta su operación con Sistema Operativo Windows XP o superior.
  - Soporta su operación con Navegadores Web 32 o 64 bits:
    - Microsoft Internet Explorer 11 o superior.
    - Mozilla Firefox 37 o superior.
    - Google Chrome Versión 37 o superior.
    - Safari versión 7.1 o superior.
- Brinda servicios criptográficos mediante alguna de las siguientes tecnologías.
  - WCAPI
  - Apple Key Chain
- Librerías propietarias de encripción y servicios criptográficos.

D. MÓDULO DE ADMINISTRACIÓN

- Cuenta con un módulo a través del cual se haga la administración de las transacciones.
- Permite la consulta y extracción de información.
- Permite la generación de reportes de acuerdo a las transacciones procesadas.
- Registra y mantiene bitácoras que permiten el monitoreo de los servicios.

E. INTERFAZ DE DESARROLLO

- Cuenta con herramientas y servicios que permiten su integración a aplicaciones propietarias o de terceros, soporta su operación en sistemas operativos tanto Microsoft Windows como UNIX.
- Soporte mandatorio a enlace seguro vía TLSv1.2.
- Cuenta con API's basados en lenguajes de programación "C", "Java" y "C#", así como, Servicios Web ofreciendo la siguiente funcionalidad:
  - Autenticación de una operación criptográfica ante el motor de firma.
  - Recuperación del documento original relacionado a partir de un número de secuencia.

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

- Retorno de evidencia criptográfica especificada, a partir de un número de secuencia.
- Solicitud de inicio de un proceso de firma multilateral.
- Autenticación de un mensaje criptográfico perteneciente a un proceso de firma multilateral.
- Estatus de un proceso de firma multilateral.
- Solicitud de digestión a firmar para un proceso de firma PDF.
- Solicitud de digestión a firmar para un proceso de firma PDF incluyendo una imagen de la firma digital del usuario.
- Solicitud de digestión a firmar para un proceso de firma PDF e incluyendo una imagen y la biometría asociada al trazo de la firma
- Finalización y obtención de constancia NOM-151 de un proceso de firma multilateral.
- Verificación de la información parametrizada corresponde al proceso de firma indicado por un identificador.
- Validación y registro de paquetes CMS firmado y con contenido.

1.21.4 Descripción técnica de Módulo CryptoServer CP5 SE 500 de Utimaco

El Utimaco CryptoServer CP5 brinda soporte a los Trusted SErvice Providers (TSPs) en el cumplimiento de los requisitos de política y seguridad definidos en varios estándares técnicos de ETSI (ETSI EN 319 401, EN 319 411, EN 319 421). Gracias a sus funcionalidades avanzadas de autorización de claves, es ideal para la creación de firmas cualificadas conforme a eIDAS y para la firma remota. Otras aplicaciones incluyen la emisión de certificados (cualificados), OCSP (Online Certificate Status Protocol) y sellado de tiempo.

El CryptoServer CP5 se basa en la plataforma de hardware CryptoServer Se Gen2 y cuenta con certificación Common Criteria de acuerdo con el Perfil de Protección (PP) eIDAS EN 419 221-5 para módulos criptográficos en servicios de confianza.

Dentro de sus principales características se encuentran:

- Ideal para aplicaciones con requerimientos de alto o bajo performance
- Administración remota extensa
- Gestión eficiente de claves y actualizaciones de firmware a través de acceso remoto.
- Automatización del diagnóstico remoto mediante SNMP (Simple Network Management Protocol).
- Simulador de software dedicado para evaluación y pruebas de integración

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, RD

Especificaciones técnicas

Algoritmos criptográficos soportados (incluida la implementación completa de NIST Suite B)
• RSA, ECDSA with NIST and Brainpool curves • ECDH with NIST and Brainpool curves • AES • CMAC, HMAC • SHA2-Family, SHA3 • Hash-based deterministic random number generator (DRG.4 acc. AIS 31) • True random number generator (PTG.2 acc. AIS 31) • Up to 3,000 RSA or 2,500 ECDSA signing operations in bulk processing mode
Plataformas soportadas
• Los sistemas operativos Windows y Linux incluyen la distribución de RedHat, SUSE y los principales proveedores de servicios de la nube que funcionan como máquinas virtuales o en contenedores
Interfaces de programación de aplicaciones (API)
• PKCS#11 • Cryptography Next Generation (CNG) • Cryptographic eXtended services Interface (CXI) – La interface de alto rendimiento de Utimacoasegura una integración fácil de las funcionalidades criptográficas con las aplicaciones del cliente
Conectividad de servidor
• Puertos duales Gigabit Ethernet (dos segmentos de red)
Cumplimiento con la seguridad
• IEC/EN 60950-1, IEC/EN 62368-1, UL, • CB Certificate, CE, FCC Class B • Security: FIPS 140-2 Level 3
Conformidad de los estándares de seguridad y medioambientales
• RoHS III, WEEE

Alta disponibilidad
• Almacenamiento sólido • Bandeja de campo, fuentes de administración intercambiables dobles
Administración supervisión
• Configuración remota • Registro de auditoría seguro. • Soporte de diagnóstico Syslog • Agente de supervisión SNMP.
Características físicas
• Dimensiones de bastidor estándar 1U 19 pulgadas: 44 x 446 x 533.4 mm • Peso: 10 kg • Voltaje de entrada: 100-240 V AC cambio automático 50-60 Hz • Consumo de potencia: 45W / 66 VA max 50W / 70 VA • Disipación del calor: 171 BTU/hora (carga completa)

Rendimiento disponible

Modelo CryptoServer CP5	**SE 500**
Rendimiento de firma RSA para longitudes de clave recomendadas por NIST	
2048 bits	800 transacciones por segundo
4096 bits	100 transacciones por segundo
Rendimiento de firma ECDSA principal para las longitudes de clave recomendadas NIST	
secp256r1	1,600 transacciones por segundo
brainpoolP256r1	1,100 transacciones por segundo
Licencias para cliente	
Incluido	2 clientes

CONSORCIO EMDOC Santo Domingo, R.D.

En caso de requerir conectar más servidores se deben contratar licencias clientes adicionales

1.21.5 Descripción técnica de Módulo CryptoServer CP5 SE 12 de Utimaco

El Utimaco CryptoServer CP5 brinda soporte a los Trusted SErvice Providers (TSPs) en el cumplimiento de los requisitos de política y seguridad definidos en varios estándares técnicos de ETSI (ETSI EN 319 401, EN 319 411, EN 319 421). Gracias a sus funcionalidades avanzadas de autorización de claves, es ideal para la creación de firmas cualificadas conforme a eIDAS y para la firma remota. Otras aplicaciones incluyen la emisión de certificados (cualificados), OCSP (Online Certificate Status Protocol) y sellado de tiempo.

El CryptoServer CP5 se basa en la plataforma de hardware CryptoServer Se Gen2 y cuenta con certificación Common Criteria de acuerdo con el Perfil de Protección (PP) eIDAS EN 419 221-5 para módulos criptográficos en servicios de confianza.

Dentro de sus principales características se encuentran:

- Ideal para aplicaciones con requerimientos de alto o bajo performance
- Administración remota extensa
- Gestión eficiente de claves y actualizaciones de firmware a través de acceso remoto.
- Automatización del diagnóstico remoto mediante SNMP (Simple Network Management Protocol).
- Simulador de software dedicado para evaluación y pruebas de integración

Compatible con la generación de claves fuera de línea y los entornos de desarrollo, a la vez que ofrece soporte completo a los algoritmos y las API.

Especificaciones técnicas

Algoritmos criptográficos soportados (incluida la implementación completa de NIST Suite B)
• RSA, ECDSA with NIST and Brainpool curves • ECDH with NIST and Brainpool curves • AES • CMAC, HMAC • SHA2-Family, SHA3 • Hash-based deterministic random number generator (DRG.4 acc. AIS 31)

CONSORCIO EMDOC Santo Domingo

• True random number generator (PTG.2 acc. AIS 31) • Up to 3,000 RSA or 2,500 ECDSA signing operations in bulk processing mode
Plataformas soportadas
• Los sistemas operativos Windows y Linux incluyen la distribución de RedHat, SUSE y los principales proveedores de servicios de la nube que funcionan como máquinas virtuales o en contenedores
Interfaces de programación de aplicaciones (API)
• PKCS#11 • Cryptography Next Generation (CNG) • Cryptographic eXtended services Interface (CXI) – La interface de alto rendimiento de Utimacoasegura una integración fácil de las funcionalidades criptográficas con las aplicaciones del cliente
Conectividad de servidor
• Puertos duales Gigabit Ethernet (dos segmentos de red)
Cumplimiento con la seguridad
• IEC/EN 60950-1, IEC/EN 62368-1, UL, • CB Certificate, CE, FCC Class B • Security: FIPS 140-2 Level 3
Conformidad de los estándares de seguridad y medioambientales
• RoHS III, WEEE
Alta disponibilidad
• Almacenamiento sólido • Bandeja de campo, fuentes de administración intercambiables dobles
Administración supervisión
• Configuración remota • Registro de auditoría seguro. • Soporte de diagnóstico Syslog • Agente de supervisión SNMP.

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

Características físicas
• Dimensiones de bastidor estándar 1U 19 pulgadas: 44 x 446 x 533.4 mm • Peso: 10 kg • Voltaje de entrada: 100-240 V AC cambio automático 50-60 Hz • Consumo de potencia: 45W / 66 VA max 50W / 70 VA • Disipación del calor: 171 BTU/hora (carga completa)

Rendimiento disponible

Modelo CryptoServer CP5	**SE 12**
Rendimiento de firma RSA para longitudes de clave recomendadas por NIST	
2048 bits	16 transacciones por segundo
4096 bits	2 transacciones por segundo
Rendimiento de firma ECDSA principal para las longitudes de clave recomendadas NIST	
secp256r1	120 transacciones por segundo
brainpoolP256r1	110 transacciones por segundo

En caso de requerir conectar más servidores se deben contratar licencias clientes adicionales

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D

2. Especificaciones de la (PKI) para la emisión de la identidad física y digital (CI/CIE)

Nuestra propuesta incluye la implantación de una infraestructura de llave pública (PKI), conforme a las especificaciones de la OACI establecidas en el Doc 9303 vigente, para emitir y revocar certificados digitales que se utilizarán para firmar electrónicamente las tarjetas electrónicas (CSCA) y para verificar tarjetas electrónicas (CVCA). La infraestructura de llave publica que describimos en esta sección será utilizada para la emitir los certificados y firmar digitalmente las identidades digitales, y poder asegurar el ciclo de vida de los certificados y las verificaciones de identidad que menciona el estándar ISO 18013-5, en cumplimiento al estándar ISO ISO 15408 (Nivel de Garantía de Evaluación de Criterios Comunes (EAL) 4+ o superior).

2.1 Especificaciones de la (PKI) para la emisión de la identidad física y digital (CI/CIE)

En esta sección procedemos a describir los componentes de la PKI necesarios para los sistemas de documentos de identidad electrónico y de la tarjeta de identificación digital:

- Tarjeta eID
  - Autenticación pasiva (PA) PKI
  - Control de acceso ampliado (EAC) PKI
  - PKI para digital
- Identificación móvil
  - ISO 18013-5 PKI

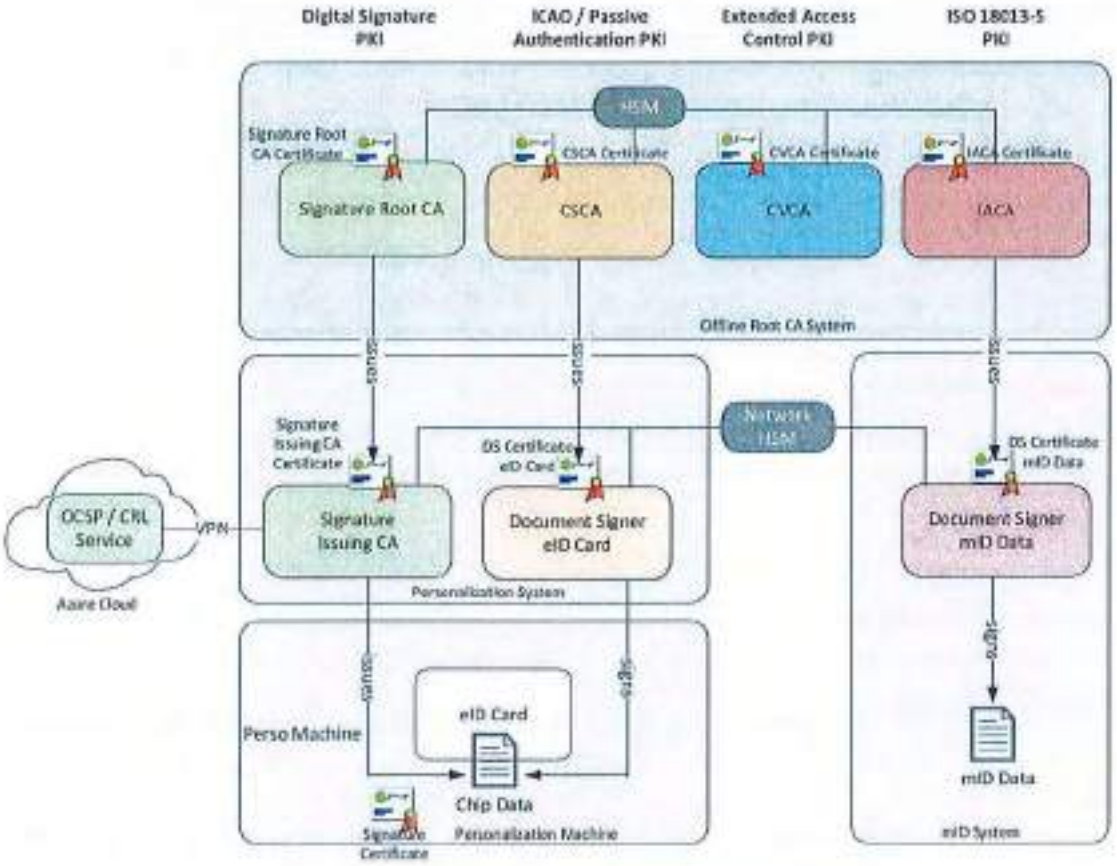


Figura1 : Visión general de la infraestructura PKI

2.2 Requisitos del sistema

El sistema propuesto soportará la personalización de documentos de identidad electrónicos y datos de identificación móviles aplicando los siguientes métodos de seguridad relacionados con la PKI:

1. Autenticación pasiva (PA)
2. Control de acceso ampliado (CAE)
3. Certificados para firmas digitales
4. ISO 18013-5 PKI

La autenticación pasiva (PA) garantiza la autenticidad e integridad de los datos almacenados en el chip del documento de identidad electrónico. Garantiza que los datos del chip proceden de la autoridad emisora legítima y que los datos no han sido manipulados. La PKI para la autenticación pasiva (PA) cumple con las especificaciones de la OACI, descritas en el documento 9303-12 y también se conoce como PKI de la OACI. Los objetos de la PKI de PA (certificados, CRL, listas maestras) deben intercambiarse con otros Estados y cargarse en sus puestos de control fronterizo. Todos los certificados emitidos y gestionados de este sistema cumplen la norma X.509 v3.

El control de acceso ampliado (EAC) garantiza la autenticidad y confidencialidad de los datos biométricos almacenados en el chip. Garantiza que los datos biométricos sólo puedan ser leídos por un lector autorizado y que el chip sea auténtico. La PKI para el control de acceso ampliado debe cumplir la directriz técnica TR-03110 de la BSI. Ambos sistemas deben proporcionar interfaces normalizadas para interactuar con el sistema de personalización de tarjetas de identidad electrónica y otros sistemas.

Los certificados de **firma** digital permiten crear firmas digitales de confianza con la tarjeta eID. El material clave para el certificado de firma se generará durante la personalización de la tarjeta y se solicitará a la PKI central un certificado conforme a la norma X.509v3 que se escribirá en la tarjeta.

El **ISO 18013-5 PKI** garantiza la autenticidad y la integridad de las identidades móviles y de los datos de los permisos de conducir móviles (mDL). Garantiza que los datos proceden de la autoridad emisora legítima y que no han sido manipulados. La PKI debe cumplir la norma ISO/IEC 18013-5:2021(en) - Personal identification - ISO-compliant driving licence - Part 5: Mobile driving licence (mDL) application.

2.3 Integración del sistema

2.3.1 Autenticación pasiva PKI

La autenticación pasiva se utiliza para garantizar la autenticidad de los datos del chip, que están estructurados en una estructura lógica de datos (LDS). Para la autenticación pasiva se necesita una autoridad de certificación de firma de país (CSCA) y un firmante de documentos (DS). La siguiente imagen muestra la vista lógica de los componentes necesarios.

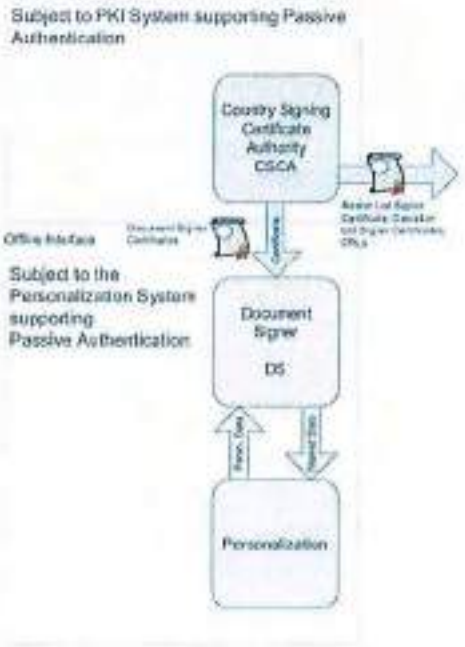


Figura2 : Infraestructura PKI para autenticación pasiva

2.3.2 Sistema PKI de control de acceso ampliado

El control de acceso ampliado (EAC) protege los datos biométricos almacenados en el chip frente a accesos no autorizados.

Las huellas dactilares se protegen mediante el protocolo EAC, tal como se especifica en BSI TR-03110 v1.11. EAC es un mecanismo de autenticación mutua basado en PKI asimétrica. Se utilizan certificados especiales verificables mediante tarjeta para definir los derechos de los terminales utilizados para la verificación de documentos.

Este sistema PKI comprende únicamente la CVCA. Al crear las claves y el certificado CVCA y escribir este anclaje de confianza en el chip, el sistema de tarjeta de identidad electrónica está preparado para su posterior ampliación mediante datos biométricos de huellas dactilares.

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

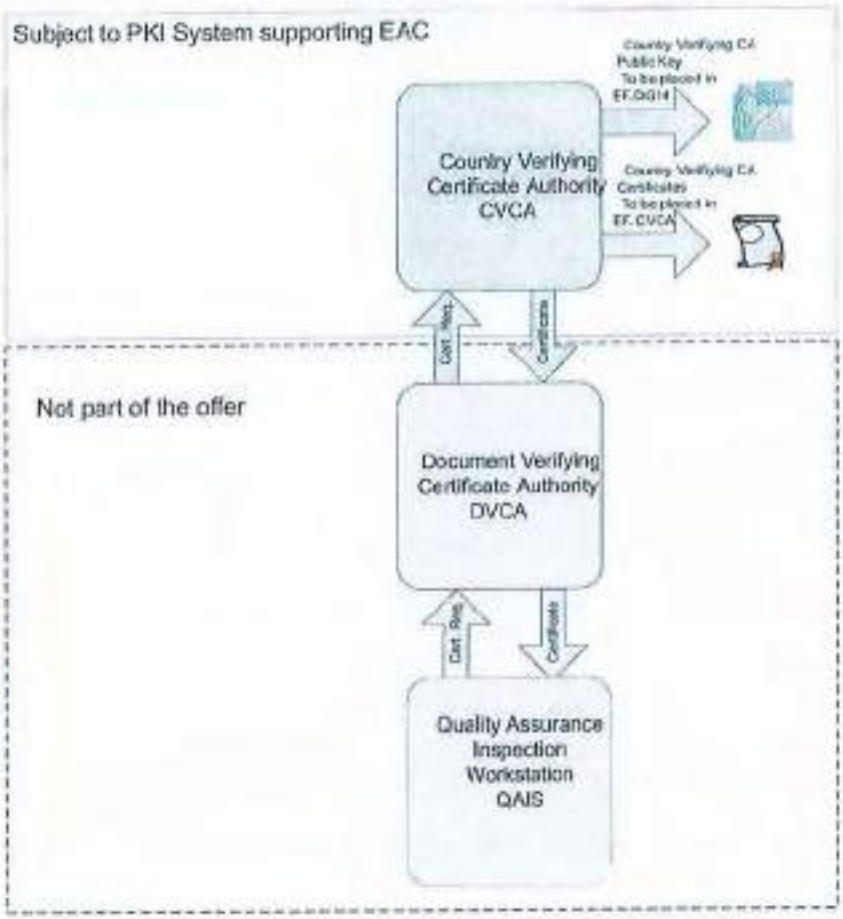


Figura3 : Infraestructura EAC para sistemas de personalización

2.3.3 Firma digital PKI

La PKI de firma digital se encarga de emitir certificados de firma para cada tarjeta eID personalizada. Los certificados están personalizados para el titular de la tarjeta. Éste puede utilizar el certificado y la clave de firma para crear firmas digitales fiables localmente en el ordenador personal o en otros dispositivos que admitan la integración del documento de identidad electrónico. La PKI consta de dos niveles: la CA raíz, que funciona fuera de línea, y la CA emisora, con conexión en línea al sistema de personalización del documento de identidad electrónico

El estado de cada certificado emitido es gestionado por el sistema CA y replicado al Certificate Status Server. A intervalos regulares se crean CRL que contienen los números de serie de todos los certificados revocados. También estas CRL se replican a este servidor. El servidor de estado de certificados publica la información a través del protocolo OCSP (Online Certificate Status Protocol) y mediante la descarga de CRL. El

Servidor de Estado de Certificados está alojado en un sistema en la nube proporcionado por el Cliente.

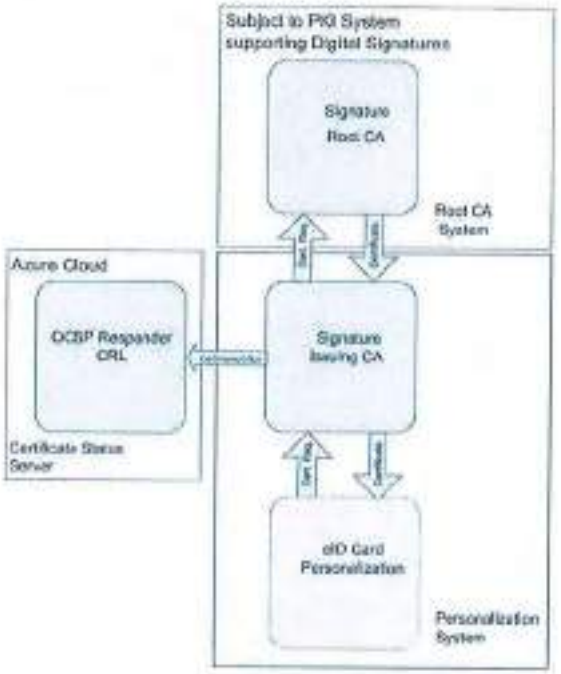


Figura4 : PKI de firma para sistemas de personalización

2.3.4 ISO 18013-5 PKI

La PKI ISO es muy similar a la PKI de autenticación pasiva. Se utiliza para garantizar la autenticidad de los datos de identidad móviles. Consta de una Autoridad Emisora Autoridad de Certificación (IACA) y un Firmante de Documentos (DS). La siguiente imagen muestra la vista lógica de los componentes necesarios.

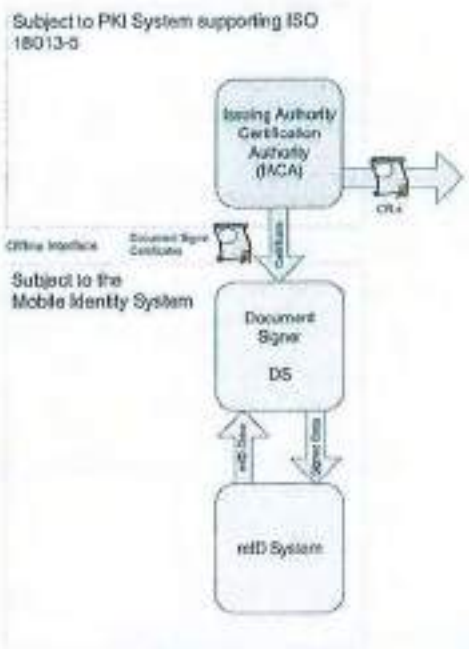


Figura5 : Infraestructura PKI para ISO PKI

2.4 Interfaces del sistema

2.4.1 Autoridad de certificación con firma de país (CSCA)

El CSCA funciona sin conexión. Todas las interfaces con otros sistemas se basan en archivos:

1. Archivos de solicitud de certificado en formato PKCS#10
2. Archivos de certificado según X509v3 en formato binario DER o ASCII PEM
3. Archivos de listas de revocación de certificados (CRL) según X509v3 en formato DER binario

2.4.2 Autoridad de certificación verificadora de países (CVCA)

El CSCA funciona sin conexión. Todas las interfaces con otros sistemas se basan en archivos:

1. Archivos de solicitud de certificado en formato PKCS#10
2. Ficheros de certificados según la norma ISO 7816 - 8 (Certificados verificables mediante tarjeta)

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

2.4.3 Firma digital PKI

Firma CA raíz

La CA Raíz de Firma funciona sin conexión. Todas las interfaces con otros sistemas se basan en archivos:

1. Archivos de solicitud de certificado en formato PKCS#10
2. Archivos de certificado según X509v3 en formato binario DER o ASCII PEM
3. Archivos de listas de revocación de certificados (CRL) según X509v3 en formato DER binario

Firma CA emisora

La CA emisora de firmas funciona en línea. Las interfaces con otros sistemas se basan en la web (REST API):

- Solicitud de certificados
- Ficheros de certificados
- Lista de revocación de certificados (CRL) según X509v3
- Información sobre el estado del certificado

Servidor de estado de certificados

El servidor de estado de certificados funciona en un servicio en la nube. Proporciona una interfaz de importación a la CA emisora para obtener información de estado y CRL y publica la información en Internet:

1. Importación de información sobre el estado de los certificados
2. Respuestas OCSP a través de http
3. Descarga de CRL a través de http

2.4.4 Autoridad emisora Autoridad de certificación (IACA)

La IACA funciona sin conexión. Todas las interfaces con otros sistemas se basan en archivos:

1. Archivos de solicitud de certificado en formato PKCS#10
2. Archivos de certificado según X509v3 en formato binario DER o ASCII PEM
3. Archivos de listas de revocación de certificados (CRL) según X509v3 en formato DER binario

2.5 Funcionalidad

2.5.1 Autoridad de certificación con firma de país (CSCA)

De acuerdo con el Informe Técnico de la OACI Doc9303 Parte 12 "Infraestructura de Clave Pública para MRTDs", esta PKI consiste en una Autoridad de Certificación de Firma de País (CSCA) como CA Raíz. La principal tarea de la CSCA es la emisión de los certificados de firmante de documentos.

El CSCA utiliza un módulo de seguridad de hardware (HSM) para la generación segura de claves, la protección de claves de hardware y la gestión del ciclo de vida de las claves, y es capaz de realizar operaciones criptográficas asimétricas con longitudes y tipos de clave conformes con la OACI.

El CSCA ofrece las siguientes funciones:

1. Generación y renovación de una clave de firma de país.
2. Generación, emisión y renovación de certificados CSCA y CSCA link autofirmados
3. Generación y emisión de certificados de firmante de documentos (X.509v3) solicitados mediante PKCS#10.
4. Generación y emisión de certificados de firmante de lista maestra (X.509v3) solicitados mediante PKCS#10.
5. Generación y emisión de certificados de firmante de lista de desviación (X.509v3) y solicitados mediante PKCS#10.
6. Generación y exportación de listas de revocación de certificados
7. Protección de claves por hardware.
8. Destrucción de las claves generadas de forma segura (tras su caducidad)

2.5.2 Autoridad de certificación de verificación de país (CVCA) .

La Autoridad de Certificación verificadora del país es el nivel raíz de la PKI de la ICAO.

La CVCA ofrece las siguientes funciones:

1. Generación y renovación de una clave de verificación de país.
2. Generación, emisión y renovación de certificados CVCA autofirmados y certificados CVCA de enlace
3. Firma de certificados de verificador de documentos para un verificador de documentos
4. Exportación de los certificados
5. Protección de claves de hardware
6. Destrucción de las claves generadas de forma segura (tras su caducidad)

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

2.5.3 Firma digital PKI

Firma CA raíz

La CA Raíz de Firma es el nivel raíz de la PKI de Firma Digital. Sirve como ancla de confianza para esta PKI.

La CA Raíz de Firma proporciona la siguiente funcionalidad:

1. Generación y renovación de una clave de CA raíz
2. Generación y emisión de certificados de CA emisora
3. Generación y emisión de CRL
4. Protección de claves por hardware.
5. Destrucción de las claves generadas de forma segura (tras su caducidad).

Firma CA emisora

La CA emisora de firmas proporciona la siguiente funcionalidad:

1. Generación y renovación de una clave de CA emisora
2. Generación y emisión de solicitudes de certificados de CA emisora
3. Importación de certificados de CA emisoras
4. Generación y emisión de CRL
5. Publicación de información sobre el estado de los certificados
6. Verificación de la identidad y autorización de los solicitantes de certificados
7. Generación de certificados de firma solicitados por el sistema de personalización
8. Protección de claves por hardware.
9. Destrucción de las claves generadas de forma segura (tras su caducidad)

Servidor de estado de certificados

El servidor de estado de certificados ofrece las siguientes funciones:

1. Importación y almacenamiento de información sobre el estado de los certificados y CRL
2. Respuesta a las solicitudes de la OSCP
3. Respuesta a las solicitudes de descarga de CRL

La CA Emisora de Firma es responsable de la producción de certificados de firma durante la personalización de las tarjetas eID. Está alojada en una máquina virtual (VM) dedicada en el hipervisor de la red interna. Para la gestión y protección de las claves privadas de la CA emisora se utilizan HSM de red. Estos HSM se compartirán con el sistema de

CONSORCIO EMDOC Santo Domingo

personalización mID, pero las claves de las CA emisoras se gestionarán en una sección (ranura) dedicada de los HSM.

Según se requiera, la CA raíz y la CA emisora utilizarán la especificación de clave RSA con un tamaño de clave de 4096 bits, los certificados de usuario (ciudadano) se emitirán con un tamaño de clave de 2048 bits. Todos los certificados se basan en las normas X.509v3 y RFC 5280. A petición también se pueden utilizar curvas elípticas según las especificaciones NIST y Brainpool.

2.5.4 Autoridad emisora Autoridad de certificación (IACA)

De conformidad con la norma ISO/IEC 18013-5:2021(en) - Personal identification - ISO-compliant driving licence - Part 5: Mobile driving licence (mDL) application, esta PKI consta de una Autoridad de Certificación Emisora (IACA) como CA Raíz. La tarea principal de la IACA es la emisión de los certificados Document Signer para las identidades digitales móviles.

La IACA utiliza un módulo de seguridad de hardware (HSM) para la generación segura de claves, la protección de claves de hardware y la gestión del ciclo de vida de las claves, y es capaz de realizar operaciones criptográficas asimétricas con longitudes y tipos de clave conformes a ISO. La principal diferencia con el CSCA según la OACI es el formato de clave utilizado en el certificado raíz.

La IACA ofrece las siguientes funciones:

1. Generación y renovación de una clave de firma de país.
2. Generación, emisión y renovación de certificados autofirmados IACA e IACA link
3. Generación y emisión de certificados de firmante de documentos (X.509v3) solicitados mediante PKCS#10.
4. Generación y exportación de listas de revocación de certificados
5. Protección de claves por hardware.
6. Destrucción de las claves generadas de forma segura (tras su caducidad).

2.6 Requisitos no funcionales

2.6.1 Disponibilidad del sistema

Todos los sistemas Root PKI, la CSCA, la CVCA, la IACA y la CA Raíz de Firma, están alojados en un sistema de servidor con HSM integrado. Después de cada operación se realiza una copia de seguridad del sistema (incluido el material de claves del HSM).

Un dispositivo de servidor redundante con HSM se mantiene en una ubicación separada. En caso de fallo del hardware primario, la copia de seguridad se restaurará en el hardware de reserva. Este sistema de copia de seguridad proporcionará una funcionalidad idéntica a la del sistema primario y garantizará la continuación sin problemas de todas las operaciones.

2.6.2 Seguridad del sistema

Todos los sistemas de la PKI raíz, la CSCA, la CVCA, la IACA y la CA raíz de firma, están alojados en un sistema de servidor aislado que funciona en un entorno de alta seguridad. Sólo se accede al sistema si es necesario realizar una operación.

El sistema admite la autenticación de dos factores con token y PIN para que los operadores inicien sesión.

Todas las conexiones de red están protegidas por cifrado mediante conexiones TLS autenticadas mutuamente.

La copia de seguridad del material clave está protegida por un conjunto de tarjetas inteligentes con PIN individuales. La restauración del material de claves requiere la presencia de un número mínimo definido de tarjetas inteligentes.

2.6.3 Despliegue del sistema

El Sistema PKI se desplegará en el Centro de Datos de la sede central, excepto el Servidor de Estado de Certificados de la PKI de Firma Digital que se alojará en un servicio en la nube.

Los módulos de seguridad de hardware (HSM) certificados según se utilizan para almacenar y gestionar de forma segura claves criptográficas y ejecutar funciones criptográficas en un entorno reforzado. El HSM de red se despliega en una disposición redundante con un segundo dispositivo conectado a la red. Los dispositivos HSM ofrecidos están certificados conforme a Common Criteria (CC) EAL4+ para sus basados en el perfil de protección eIDAS EN 419 221-5 [4].

Se utiliza un sistema de servidor dedicado con PCI HSM integrado para alojar la CSCA fuera de línea, la CVCA, la IACA y la CA raíz de firma.

Se desplegará un sistema de prueba para los distintos sistemas PKI en un entorno independiente.

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

2.7 Hardware y software del sistema PKI

En este capítulo se enumeran todos los componentes relevantes del sistema. Este capítulo resume los componentes de hardware y software necesarios asignados a los bloques de construcción definidos anteriormente. Los siguientes componentes de hardware del sistema PKI se consideran :[1]

No.	Cantidad	Artículo	Comentario
1	2	Sistema de servidor montable en bastidor de 19 pies, ranura PCIe de tamaño completo (para la tarjeta HSM	Requisitos mínimos: 1 CPU, 16 GB RAM, 200GB HD
2	2	Conmutador de red	Vinculación del sistema CA con la estación de trabajo de administración
3	1	Puesto de administración	PC o portátil con Windows
4	10	Fichas criptográficas USB	Para material de claves y certificados de autenticación de clientes
5	1	Disco duro USB	Copiar archivos de copia de seguridad del sistema sin conexión
6	2	Utimaco CryptoServer CP5 Se52 PCIe, CC certificado según EN419221-5	Para el sistema CA raíz
7	2	Utimaco CC eIDAS en CryptoServer HSM de red de uso general SecurityServer Se100 LAN V5	Para sistemas CA emisores

Se consideran los siguientes componentes de software del Sistema PKI:

No.	Cant.	Artículo	Observaciones
1	1	Licencia del software VeriKEY Certificate Manager CSCA/CVCA/IACA	Licencia de Veridos para el manejo de aplicaciones sw CSCA, CVCA e IACA

[1] Bastidores, SAI y otros componentes de infraestructura no enumerados aquí

2	1	Licencia del software Starfish PKI	Licencia para el manejo de CA raíz de firma y CA emisora
3	1	Middleware AET SafeSign	Para la integración de tokens Crypto USB en el puesto de trabajo de administrador.

Referencias:

[1] Doc. 9303 de la OACI, Documentos de viaje legibles por máquina, octava edición 202, Parte 12: Infraestructura de clave pública para MRTD.

[2] BSI TR-03110, Mecanismos avanzados de seguridad para documentos de viaje legibles por máquina

[3] ISO/IEC 18013-5:2021(en) - Personal identification - ISO-compliant driving licence - Part 5: Mobile driving licence (mDL) application (Identificación personal - Permiso de conducción conforme a ISO - Parte 5: Aplicación de permiso de conducción móvil)

[4] CSN EN 419221-5, Perfiles de protección para módulos criptográficos TSP - Parte 5: Módulo criptográfico para servicios de confianza.

EMDOC
CONSORCIO

ÍTEM IV. PROPUESTA TÉCNICA PARA LA TARJETA DE IDENTIDAD DIGITAL

PARA LA CONTRATACIÓN DE LA EMPRESA QUE SE ENCARGARÁ DE SUPLIR LOS EQUIPOS, MATERIALES Y SERVICIOS PARA LA IMPRESIÓN DE LA CÉDULA DE IDENTIDAD Y ELECTORAL (CIE) Y CÉDULA DE IDENTIDAD (CI)

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

9

EMDOC CONSORCIO

CONTENIDO

1 Respuesta técnica a PUNTO IV - ESPECIFICACIONES TÉCNICAS TARJETA DE IDENTIDAD DIGITAL 3

1.1. Resumen de la solución 3

1.2. Plataforma de microservicios de identificación digital 4

1.3. Autenticación 7

1.4. Arquitectura de confianza cero 7

1.5. Verificación y validación de la identidad 9

1.6. Aprovisionamiento y desaprovisionamiento de usuarios 9

1.7. Experiencia de usuario y autoservicio 10

2 Arquitectura del sistema 14

2.1. Integración de microservicios con Feign Client y plantillas 14

2.2. Normas de seguridad de la plataforma: 15

2.3. Consideraciones generales sobre el hardware para dimensionar la infraestructura 17

2.4. Consideraciones adicionales 19

2.5. Método de despliegue: Multi-Host On-Premise - Contenedores Docker 19

2.6. Proceso de actualización local para Docker 21

2.7. Mantenimiento de la Plataforma 23

2.8. Análisis de interfaces y plan de pruebas para interfaces de comunicación 25

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

EMDOC

1 Respuesta técnica a PUNTO IV - ESPECIFICACIONES TÉCNICAS TARJETA DE IDENTIDAD DIGITAL

1.1. Resumen de la solución

La plataforma ofrece un ecosistema de identidad digital interoperable que garantiza el acceso seguro a servicios tanto públicos como privados. Un elemento clave de esta solución es la Cédula Digital, que cuenta con un monedero móvil y un verificador móvil con certificación ISO 18013-5, que supera los requisitos de seguridad mediante una sólida validación criptográfica. El sistema de identidad digital está diseñado para ser modular, escalable y capaz de adaptarse a una demanda fluctuante. Aprovecha la tecnología API REST en entornos de nube pública o privada y emplea credenciales verificables (VC) del W3C para una autenticación digital segura. La plataforma integra funciones esenciales de ciberseguridad, como la lectura electrónica de chips y la verificación facial 1 a 1 para dispositivos compatibles, lo que garantiza un marco de alta seguridad y una verificación de identidad sin fisuras. Además, los dispositivos móviles incorporan medidas de protección contra la ingeniería inversa, la manipulación del código y el acceso no autorizado.

Tanto la aplicación móvil del titular como la del verificador son compatibles con iOS y Android y cuentan con la certificación **FIME** para 18013-5 . Funciones configurables que ofrecen compatibilidad con funciones de seguridad como la autenticación multifactor (AMF) y, previa aprobación del usuario, la verificación facial compatible con el dispositivo para acceder al monedero de identificación del titular. La activación remota de las identidades digitales se facilita a través de enlaces temporales enviados por correo electrónico o mensaje de texto, con períodos de caducidad controlados para mejorar la seguridad. Además, admite la visualización de datos fuera de línea para mejorar la accesibilidad de los casos de uso de verificación por parte del gobierno o las fuerzas de seguridad.

La plataforma se desplegará como un entorno de alta disponibilidad con capacidades de conmutación por error que limitan el tiempo de inactividad a no más de cinco minutos. La plataforma basada en microservicios será compatible con la interoperabilidad y la escalabilidad, lo que permitirá una integración perfecta con los servicios existentes y futuros.

Un sistema de identidad digital seguro, escalable y eficiente que pueda desplegarse in situ o en la nube que mantenga la confianza pública y mejore la accesibilidad mediante el cumplimiento de las normas mundiales de seguridad e interoperabilidad proporcionará la infraestructura sólida y preparada para el futuro que busca el honorable JCE.

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

EMDOC

1.2. Plataforma de microservicios de identificación digital

- **Emisión de tarjetas de identidad digital (CD) y gestión de perfiles de usuario:** La plataforma permite a la JCE crear procesos personalizados de registro de usuarios y gestión de perfiles aprovechando el requisito de integración de su actual sistema central de gestión de tarjetas. Esto se hace mediante la configuración de los recorridos de identidad, personalizando los flujos de incorporación, inscripción, adjudicación, autenticación y autorización. Esta flexibilidad permite al JCE adaptarse a diversos requisitos normativos y políticas internas . La plataforma también permite la incorporación de un sistema integral de gestión del ciclo de vida de las credenciales digitales. Esto soportará el ciclo de vida completo de las credenciales, incluyendo su emisión, activación y revocación. También admite el registro de los eventos de acceso de cada credencial para garantizar la trazabilidad y la seguridad. También proporciona las aplicaciones o interfaces necesarias para apoyar la integración e implantación de nuevas soluciones.

- **Visión general de la plataforma:**
  La plataforma multiarrendamiento utiliza una arquitectura de microservicios, que se divide en unidades modulares y escalables, cada una de las cuales se encarga de funciones específicas.

  - Entre sus principales servicios figuran:
    - **Pasarela WEB-API**
    - **Gestión de la orquestación**
    - **Gestión de usuarios**
    - **Gestión de credenciales**
    - **Gestión de informes**
    - **Servicio de notificación**
    - **Servicio de verificación biométrica**

  - **Gestión de identidades y accesos:**
    La plataforma cuenta con un proveedor de identidades (IdP) integrado que autentica y autoriza a los usuarios para acceder de forma segura a los servicios y aplicaciones de la plataforma. Puede emitir y gestionar identidades de usuario, como Mobile Wallets, e integrarse con proveedores de identidad externos como OpenID Connect (OIDC), Security Assertion Markup Language (SAML) o Active Directory (AD).

    La plataforma VerIGO MobileID contiene múltiples plataformas de interfaz como SAML, OIDC, LDAP y varios protocolos de bases de datos. Realizaremos la interfaz basándonos en las interfaces elegidas de JCE.

Características principales:

- **Autenticación centralizada:** Control de acceso unificado en toda la organización.

- **Políticas personalizadas:** Se alinea con las políticas de seguridad de tu organización.

- **Autenticación multifactor (MFA):** Añade una capa adicional de seguridad a los servicios y aplicaciones de la plataforma.

- **Compatibilidad con la API REST:**
  La plataforma expone una API REST que permite a los desarrolladores interactuar con sus servicios mediante programación. La API REST está diseñada para ser:
  - **Sin estado:** Cada petición API del cliente contiene toda la información necesaria para que el servidor la entienda y procese, haciendo que el servicio sea escalable y fiable.
  - **Orientada a recursos:** La API está estructurada en torno a recursos como usuarios, credenciales e informes, a los que se puede acceder y manipular mediante métodos HTTP estándar (GET, POST, PUT, DELETE).
  - **Segura:** Todas las interacciones a través de la API REST están protegidas mediante HTTPS, lo que garantiza el cifrado de los datos en tránsito.

- **Soporte de aplicaciones heredadas:**
  Las aplicaciones heredadas sin soporte OAuth2-OIDC o SAML aún pueden integrarse con la plataforma utilizando Claves de Acceso API para el acceso seguro a recursos HTTPS.

- **Gestión del ciclo de vida del DNI digital**

  - **Creación y modificación de usuarios**

    - La plataforma ofrece un portal administrativo fácil de usar para crear y gestionar perfiles de usuario. Admite trayectos de usuario personalizables, lo que permite controles de acceso flexibles basados en funciones para administradores, operadores, ciudadanos y usuarios temporales. El JCE puede adaptar estos itinerarios a sus políticas y requisitos específicos actuales y futuros, incluida la activación remota mediante SNS para enviar enlaces de tiempo limitado por correo electrónico o SMS, garantizando la seguridad con un método de autenticación de dos factores (2FA) PIN y verificación facial como mínimo.

- Aprovisionamiento automatizado basado en eventos de registro, flujos de trabajo o secuencias de comandos.
- Puede admitir la definición de atributos de identidad personalizados y el control de las correspondencias y los valores de los datos.
- La plataforma se integra perfectamente con sistemas externos a través de un sólido marco de API. Esta integración permite sincronizar los datos de usuario, la autenticación y los procesos de autorización con otras aplicaciones y servicios. Al adherirse a estándares del sector como las API RESTful, la plataforma garantiza la interoperabilidad y la flexibilidad
- Desaprovisionamiento automatizado basado en eventos o flujos de trabajo específicos.

- **Soporte para el ciclo de vida completo de las credenciales, incluida la emisión, activación y revocación**
- **Desduplicación de ID de usuario**
  - Mecanismos sólidos de eliminación de duplicados para evitar la duplicación de ID de usuario.
  - Algoritmos avanzados de concordancia para identificar posibles duplicados.
- **Alertas y notificaciones**
  - VerIGO MobileID ofrece la posibilidad de proporcionar notificaciones a través del servicio SNS (notificaciones push móviles en la aplicación o en la pantalla de inicio del dispositivo, así como por correo electrónico). La forma, el contenido y la audiencia de los mensajes tendrían que definirse conjuntamente con JCE.
  - En lo que respecta a las notificaciones de ID Wallet durante la activación del dispositivo Según la norma ISO/IEC 180[illegible] 5, Veridos desea destacar que un código de barras esta destinado únicamente a la activación del dispositivo.
    - Cuando un ciudadano abre su aplicación, se le presenta la imagen de su credencial digitalizada. Desde esta pantalla puede ver sus propios datos o presentar la credencial de forma verificable. Desde la perspectiva del ciudadano, la transacción de identidad

se inicia con su entrada a través del icono "Permitir inspección". La participación del dispositivo facilita la comunicación entre el dispositivo del titular y el dispositivo del verificador a través de un canal de comunicación seguro . Esta comunicación se realiza mediante tecnología BLE o NFC. Tras la conexión del dispositivo, el titular recibirá una lista de los atributos que se solicite compartir como parte de la transacción de identidad. En esta fase, el titular puede dar su consentimiento o revocarlo en cualquier momento. Esto se aplica tanto a la transmisión de la credencial completa como a los atributos de identidad individuales; por ejemplo, un usuario puede negarse a compartir su fecha de nacimiento exacta y confirmar que tiene más de 18, 19 o 21 años.

1.3. Autenticación

Autenticación basada en el riesgo

- Autenticación adaptativa: Ajuste el nivel de autenticación necesario en función de factores de riesgo, como la dirección IP, el tipo de dispositivo o el comportamiento del usuario.

Inicio de sesión único (SSO) - (SAML, OAuth, OpenID Connect)

- Estándares compatibles para facilitar la integración de las organizaciones, la integración de las partes confiantes y otros casos de uso para permitir el acceso sin problemas a múltiples aplicaciones con un único inicio de sesión.

1.4. Arquitectura de confianza cero

Es un modelo de seguridad que asume que ningún usuario o dispositivo es intrínsecamente fiable. Requiere la verificación continua de usuarios y dispositivos antes de conceder acceso a los recursos.

Los principios clave de la plataforma incluyen:

- No confíe nunca, verifique siempre: Valida continuamente la identidad del usuario y el estado del dispositivo.
- Modelo de acceso de mínimo privilegio: Conceder a los usuarios sólo los permisos mínimos necesarios.
- Microsegmentación: Aísle los segmentos de la red para limitar el impacto de posibles brechas.

CONSORCIO EMDOC
EMDOC CONSORCIO
Santo Domingo, RD

- Supervisión y registro continuos: Supervise el tráfico de red y la actividad de los usuarios en busca de anomalías.

Consideraciones adicionales

- Experiencia del usuario: Garantice una experiencia de autenticación fluida y fácil de usar.
- Mejores prácticas de seguridad: Adhiérase a las normas y mejores prácticas del sector para una autenticación segura.
- Evaluaciones periódicas de la seguridad: Realice evaluaciones de seguridad periódicas para identificar y mitigar vulnerabilidades.
- Plan de respuesta a incidentes: Disponga de un plan de respuesta a incidentes bien definido para hacer frente a las brechas de seguridad.
- Al adoptar un modelo de credenciales sin contraseña y resistente al phishing, las organizaciones pueden mejorar significativamente su postura de seguridad y proteger los datos confidenciales.
- Datos de identificación de la persona (DIP)
  - Los Datos de Identificación Personal (DIP) son la forma más importante y segura de credenciales verificables. Los PID son expedidos directamente por las autoridades gubernamentales y sirven como la más fundamental de la identidad de una persona. Los PID son credenciales emitidas por el gobierno que vinculan a una persona con su estatus legal.
  - En el caso de las personas jurídicas, los PID suelen denominarse LPID (Legal Person Identification Data, datos de identificación de la persona jurídica), que son cruciales para interacciones seguras y verificadas entre servicios públicos y privados.
  - Ejemplos:
    - Documento de identificación móvil (mID) expedido por el Gobierno, credencial digital de viaje (DTC), permiso de conducir móvil (mDL).
    - LPID - certificado de registro de empresa que acredita la personalidad jurídica.

Autoservicio de restablecimiento de contraseña:

- Restablecimiento de contraseña iniciado por el usuario a través de un proceso seguro que implica la autenticación multifactor.
- Bloqueo automático de la cuenta tras varios intentos fallidos de inicio de sesión.
- Procedimientos de desbloqueo de cuentas, incluido el restablecimiento de la contraseña o la intervención administrativa.

1.5. Verificación y validación de la identidad

- **Verificación de la prueba de identidad**
  - Verificación de documentos de identidad mediante procesos manuales o automatizados aprovechando los servicios existentes de la organización, utilizando los servicios IDV integrados o integrando servicios ahora en el futuro mediante API o el SDK de ID Wallet.
- **Autenticación biométrica**
  - Integración con tecnologías de autenticación biométrica (por ejemplo, reconocimiento facial, huella dactilar) para mejorar la seguridad.
  - La detección de actividad o la integración con tecnologías existentes o emergentes pueden aplicarse para mitigar los ataques de suplantación de identidad.

1.6. Aprovisionamiento y desaprovisionamiento de usuarios

- **Aprovisionamiento automatizado**
  - Creación automática de cuentas de usuario basada en reglas y flujos de trabajo predefinidos.
  - Integración con sistemas organizativos mediante API basadas en estándares, como las API RESTful, para sincronizar los datos de los usuarios.
- **Desaprovisionamiento automático**
  - Eliminación automática de cuentas de usuario en caso de rescisión u otros eventos específicos.
  - Al darse de baja el usuario, el sistema borrará de forma segura los datos personales, revocará los privilegios de acceso y archivará la información necesaria. Las políticas de conservación y supresión de datos se revisarán

CONSORCIO EMDOC EMDOC CONSORCIO

periódicamente para garantizar el cumplimiento de la normativa.

- **Borrado de datos**: Borrado seguro de todos los datos personales asociados al usuario, incluidos, entre otros:
  - Información personal identificable (IPI)
  - Datos sensibles (por ejemplo, historiales médicos, información financiera)
  - Preferencias y ajustes del usuario

- **Recuperación de recursos**: Revocación de todos los privilegios de acceso y eliminación de los permisos de usuario de sistemas y aplicaciones.

- **Conservación de registros de auditoría**: Conservación de los registros de auditoría necesarios con fines de cumplimiento y seguridad, al tiempo que se anonimiza o redacta la información sensible.

- **Archivo de datos**: Archivar los datos necesarios para fines legales o reglamentarios, garantizando medidas de seguridad y controles de acceso adecuados.

- **Verificación del cumplimiento**: Revisión y actualización periódicas de las políticas de conservación y eliminación de datos para alinearlas con la evolución de la normativa (por ejemplo, GDPR, CCPA, HIPAA).

Siguiendo estas buenas prácticas, la Plataforma garantizará que los datos de los usuarios se traten de forma responsable y segura, minimizando los riesgos potenciales y manteniendo el cumplimiento de la normativa aplicable.

1.7. Experiencia de usuario y autoservicio

La Plataforma ha sido diseñada para ser lo más intuitiva y sencilla posible. Maximiza la facilidad de uso, al tiempo que mantiene el máximo nivel de seguridad y privacidad.

- **Interfaz fácil de usar**
  - Interfaz de usuario intuitiva para facilitar la navegación y la realización de tareas.
- **Experiencia personalizada**

- Experiencias de usuario personalizadas en función de sus funciones y preferencias.
- Recomendaciones y notificaciones contextuales.

- **Verificación y validación de la identidad**
  - Procesos sólidos de verificación de la identidad, incluida la validación de documentos, la autenticación biométrica y la compatibilidad con los dispositivos requeridos por el cliente.
  - Integración con proveedores de identidad externos para una autenticación sin fisuras.
  - Mecanismos de autenticación y autorización basados en el riesgo para garantizar la seguridad.
- **Billetera digital**
  - El identificador visual configurable utiliza un SVG cifrado y las credenciales se generan en el momento de la emisión: digitalmente son únicas. La información visualmente oculta (como el IPI) puede entregarse en el momento de la emisión. La orientación de la identificación visual es configurable, incluidos los elementos de la interfaz de usuario
  - Almacenamiento seguro del carné de identidad digital (CD)
  - Fácil acceso a los documentos a través de la aplicación móvil.
  - Soporte para NFC, verificación basada en código QR y fichas digitales de un solo uso de serie con el monedero móvil.
  - Política de inicio de sesión de dispositivos configurable, los dispositivos también pueden limitarse en función de la política establecida por el JCE a medida que evolucionan los requisitos.
  - Admite procesos de cambio de dispositivo basados en flujos de trabajo, incluidos el inicio, la verificación y la autenticación de usuarios, la validación de dispositivos y las actualizaciones de perfiles. Prioriza la seguridad mediante una autenticación sólida y medidas de protección de datos.
  - *ISO 18013-5 Certificado por FIME*
  - VeriGO MobileID admite tanto el modo de recuperación por servidor como por dispositivo. La posibilidad de que los ciudadanos presenten su información para su inspección y de que las partes de confianza verifiquen dicha información

incluso sin conexión a Internet es una característica de VeriGO MobileID definida en ISO/IEC 18013-5. El periodo de validez de una credencial en modo fuera de línea (recuperación del dispositivo) está sujeto a las normas empresariales de JCE y se aclarará durante la fase de proyecto.

- Una característica estándar de VeriGO MobileID para priorizar la privacidad y la comodidad del usuario. La minimización de datos definida por el usuario es un principio básico de la especificación ISO/IEC 18013-5. Tras la activación del dispositivo, se solicitará al titular una lista de los atributos que se desea compartir como parte de la transacción de identidad. En esta fase, el titular puede dar su consentimiento o revocarlo en cualquier momento. Esto se aplica tanto a la transmisión de la credencial completa como a los atributos de identidad individuales; por ejemplo, un usuario puede negarse a compartir su fecha de nacimiento exacta y confirmar que tiene más de 18, 19 o 21 años.

- Todos los datos presentados se firmarán electrónicamente para garantizar que terceros puedan validar la integridad y el origen de los datos proporcionados por el ciudadano. Esto forma parte de la norma ISO/IEC 18013-5 que Veridos cumple.

- Las credenciales se almacenan en un elemento seguro (enclave). Cuando se instala la aplicación VeriGO MobileID, se comprueba si el dispositivo móvil está rooteado o jailbreakeado antes de proceder a la instalación. Las aplicaciones móviles están firmadas digitalmente y ofuscadas - esto significa que todo el código ha sido codificado intencionadamente impidiendo cualquier intento de ingeniería inversa . Cada vez que VeriGO MobileID se comunica con el servidor a través de TLS, la comunicación se cifra sistemáticamente.

- Una representación digital de la credencial puede verse después de que el usuario abra VeriGO MobileID y haya completado los requisitos 2FA. Cuando, tras completar los requisitos 2FA, un ciudadano abre su aplicación, se le presenta una imagen de su credencial digitalizada. Desde esta pantalla puede ver sus propios datos o presentar la credencial de forma verificable. Desde la perspectiva del ciudadano, la transacción de identidad se inicia con su entrada a través del icono "Permitir inspección".

- **Verificador móvil:**
  - Los verificadores, como los funcionarios, dependen actualmente de comprobar la identificación de un usuario con un documento físico. Con el verificador móvil, el funcionario puede confirmar la identidad de un usuario a través de su dispositivo móvil.
  - Utiliza métodos rigurosos y exhaustivos para verificar los documentos de identificación de un usuario. Los verificadores pueden estar seguros de que los documentos son auténticos y válidos.
  - Se obtiene el consentimiento de los usuarios para garantizar que comprenden y aceptan compartir sólo la información necesaria con el proveedor de servicios.
  - Verificación basada en NFC: Verificación offline de credenciales de identidad mediante tecnología NFC.
  - Verificación por código QR configurable: Verificación offline mediante códigos QR generados y almacenados en el dispositivo del usuario.
  - Tokens digitales de un solo uso: Verificación fuera de línea mediante tokens de un solo uso para la verificación segura de la identidad en ubicaciones de terceros.
  - *ISO 18013-5 Certificado por FIME*
- **Registro y auditoría**
  - Registro y auditoría exhaustivos de todas las actividades de los usuarios y eventos del sistema
  - Supervisión de la salud y la seguridad del sistema.
- **e-KYC y renovación**
  - Procesos automatizados de e-KYC para verificar periódicamente la identidad de los usuarios.
  - Recordatorios puntuales de renovación y expiración de documentos.
- **Notificaciones configurables**
  - Admite notificaciones personalizables JCE para satisfacer requisitos específicos del usuario o del sistema

- El JCE de apoyo debe registrar los eventos de acceso para cada credencial, garantizando la trazabilidad y mejorando la seguridad.

- API y SDK disponibles para la plataforma MobileID

2 Arquitectura del sistema

2.1. Integración de microservicios con Feign Client y plantillas

Aprovechando la potencia de Feign, la plataforma simplifica las complejas interacciones API, mejora la legibilidad del código y la fiabilidad general del sistema. La solución propuesta proporcionará una capa de integración sin fisuras, permitiendo una comunicación eficiente y el intercambio de datos entre microservicios y sistemas heredados

Visión general de alto nivel del proceso:

- **Definir interfaces de cliente falsas:**
  - Cree interfaces Java para representar las API del servicio remoto.
  - Anote los métodos de la interfaz con los métodos HTTP apropiados (GET, POST, PUT, DELETE) y los parámetros de solicitud/respuesta.

- **Crear plantillas falsas:**
  - Defina plantillas para encapsular patrones comunes en las llamadas a la API, como la construcción de URL, cabeceras y parámetros de consulta.
  - Utilice variables de plantilla para parametrizar las solicitudes, haciéndolas flexibles y reutilizables.
- **Configurar clientes falsos:**
  - Especifique la URL base del servicio remoto.
  - Configure la gestión de errores, los reintentos y otros ajustes del lado del cliente.
  - Integración con mecanismos de equilibrio de carga para distribuir el tráfico entre varias instancias del servicio remoto.
- **Invocación al Servicio:**
  - Inyecte clientes Feign en sus microservicios
  - Invoca servicios remotos llamando a métodos de la interfaz de cliente Feign, pasando los parámetros necesarios a las plantillas.

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, RD

- Feign gestiona las peticiones HTTP subyacentes, incluida la construcción de URL, la serialización de petición/respuesta y la gestión de errores.

Principales ventajas de utilizar el cliente falso y las plantillas:

- **Consumo simplificado de la API**: Feign abstrae la complejidad de las peticiones HTTP.
- **Enfoque declarativo**: Define las API mediante interfaces Java, lo que mejora la legibilidad y el mantenimiento del código.
- **Reutilización**: Las plantillas pueden reutilizarse en varios clientes Feign, lo que reduce la duplicación de código.
- **Flexibilidad:** Personaliza fácilmente las peticiones pasando parámetros a las plantillas.
- **Mecanismos de tratamiento de errores y reintentos:** Soporte integrado para la gestión de errores, reintentos y disyuntores.
- **Equilibrio de carga:** Integración con mecanismos de equilibrio de carga para un rendimiento óptimo.

Al aprovechar Feign Client y las plantillas, la plataforma puede integrar eficazmente microservicios con sistemas locales, fomentando la modularidad, la escalabilidad y la capacidad de mantenimiento.

2.2. Normas de seguridad de la plataforma:

Normas de seguridad de la plataforma VenGO MobileID

Norma de seguridad	Protocolos
Clave simétrica	AES: 128, 256 Longitudes de clave configurables.
Clave asimétrica	RSA: 2048, 4096 Longitudes de clave configurables.
	ECC: 256, 384, 521 Longitudes de clave configurables.
Resumen de mensajes	SHA: 256 384, 512 Bits configurables.
mID/mDL Estándar	Permiso de conducir conforme a ISO/IES 18013-5: ISO.
Código de autenticación del mensaje	HMAC: SHA-256 SHA-384, SHA-512 Bits configurables.

Https seguros	TLS: v1.3 v1.2 están configurados con suites de cifrado fuertes.
Autenticación y verificación multifactoriales	Orden precedente: FIDO2 – PUSH – PKI – OTP – Código QR

Directrices de seguridad de la plataforma VeriGO MobileID

Normas	Acciones
Datos cifrados en tránsito	Activar el cifrado de la capa de transporte TLS 1.2 o TLS 1.3
SSO MFA y verificación	Habilite la autenticación multifactor: FIDO2, PUSH, PKI, OTP, código QR
Proteger el acceso a aplicaciones y puntos finales	Es obligatorio acceder a todos los puntos finales y a la aplicación mediante tokens JWT válidos a través de OAUTH o claves de acceso a la API.
Controles de acceso basados en funciones	Aplicar políticas y gobernanza para limitar el acceso de los usuarios en función de la función asignada es fundamental.
Desconfiguración de la seguridad	Aplique las configuraciones sólo después de revisarlas y aprobarlas mediante la comprobación de cumplimiento de la seguridad.
Prevención de la pérdida de datos	Copias de seguridad frecuentes en clintas para mitigar la pérdida de datos y respaldar el BCP (Business Continuity Plan)
Comprobación de seguridad antes de la implantación	Asegure la infraestructura y la red antes del despliegue VPN, ubicación de sesión controles SSH
Registro y control	Habilitar el registro de aplicaciones que ayudaría en caso de compromiso.

Tal y como se define en la norma ISO/IEC 18013-5, VeriGO MobileID proporciona canales de comunicación cifrados para las transacciones de identidad a través de NFC y BLE. Tanto la autenticación de datos como el cifrado de sesiones se realizan utilizando ES256 (ECDSA con SHA-256), ES384 (ECDSA con SHA-384) y AES-256.

Cifrado de datos: Todos los datos transferidos hacia y desde la aplicación son seguros y no pueden ser accedidos por partes no autorizadas, incluyendo Veridos. La aplicación sólo recoge y almacena la

información esencial necesaria para su funcionamiento, evitando la recopilación innecesaria de datos.

- Se facilitan políticas de privacidad transparentes y comprensibles que detallan cómo se utilizan, almacenan y protegen los datos de los usuarios.
- El derecho al olvido: permite a los usuarios que lo soliciten borrar completamente sus datos de la aplicación.
- Dentro de la aplicación, los datos del usuario sólo se almacenan durante el periodo necesario para el fin con el que se recogieron.

Autenticación segura: Implanta mecanismos de autenticación fuertes, como la autenticación multifactor.

Control de acceso: Aplique estrictos controles de acceso para proteger los datos confidenciales.

Auditorías de seguridad periódicas: Realice auditorías de seguridad periódicas para identificar y abordar las vulnerabilidades.

Cumplimiento de la normativa: Adherirse a la normativa pertinente sobre protección de datos (por ejemplo, GDPR, CCPA).

2.3. Consideraciones generales sobre el hardware para dimensionar la infraestructura

Servidores:

- **Servidores de aplicaciones**
  - CPU de alto rendimiento de 64 núcleos (por ejemplo, Intel Xeon o AMD EPYC)
  - RAM (por ejemplo, 128 GB o más)
  - Alta capacidad de almacenamiento rápido SSD para archivos de aplicaciones y datos con al menos 500 GB de almacenamiento.
  - Equilibradores de carga para distribuir el tráfico entre varios servidores
- **Servidores de bases de datos**
  - CPU de alto rendimiento de 32 núcleos (por ejemplo, Intel Xeon o AMD EPYC)

CONSORCIO EMDOC EMDOC Santo Domingo, R.D.

- RAM (por ejemplo, 64 GB o más)
- Alta capacidad de almacenamiento rápido SSD para archivos de aplicaciones y datos con al menos 1 TB de almacenamiento.
- Técnicas de optimización de bases de datos (por ejemplo, indexación, optimización de consultas)

- **Servidores de autenticación**
  - CPU de alto rendimiento de 16 núcleos (por ejemplo, Intel Xeon o AMD EPYC)
  - RAM (por ejemplo, 32 GB o más)
  - Alta capacidad de almacenamiento rápido SSD para archivos de aplicaciones y datos con al menos 100 GB de almacenamiento.
  - Técnicas de optimización de bases de datos (por ejemplo, indexación, optimización de consultas)

Infraestructura de red:

- **Red de alta velocidad**
  - Red Gigabit Ethernet o 10GbE para una transferencia de datos de alto rendimiento
  - Conmutadores y enrutadores de red con baja latencia y gran ancho de banda
- **Equilibradores de carga:** Distribuye el tráfico de red o de aplicaciones entre varios servidores para mejorar el rendimiento, la fiabilidad y la escalabilidad.
- **Cortafuegos:**
  - Proteger el sistema de accesos no autorizados y ciberamenazas.

CONSORCIO EMDOC EMDOC CONSORCIO

Almacenamiento de alto rendimiento

- Unidades SSD o NVMe para un acceso rápido a los datos
- Configuraciones RAID para redundancia y rendimiento

Copias de seguridad y recuperación en caso de catástrofe

- Copias de seguridad periódicas para garantizar la integridad de los datos y la continuidad de la actividad

- Plan de recuperación en caso de catástrofe para minimizar el tiempo de inactividad en caso de avería

2.4. Consideraciones adicionales

Almacenamiento en caché: Implemente mecanismos de almacenamiento en caché para reducir la carga de la base de datos y mejorar los tiempos de respuesta.

Pruebas de carga: Realice pruebas de carga rigurosas para identificar cuellos de botella en el rendimiento y optimizar el sistema.

Supervisión y alertas: Configure herramientas de supervisión para realizar un seguimiento del rendimiento del sistema y abordar los problemas de forma proactiva.

Seguridad: Aplique medidas de seguridad sólidas para proteger los datos confidenciales de los usuarios.

Escalabilidad: Diseñe el sistema de forma que sea escalable para adaptarse al crecimiento futuro.

2.5. Método de despliegue: Multi-Host On-Premise - Contenedores Docker

Visión general

Este método de despliegue utiliza servidores físicos o virtuales en un centro de datos, extendiendo la contenedorización a múltiples hosts. Este enfoque proporciona un mayor control y optimización, ya que las tareas se ejecutan localmente antes de enrutarse en línea.

Alcance y escalabilidad:

Para llevar a cabo esta implantación, se necesitarán los siguientes servidores (virtuales o físicos):

1. **Servidor de bases de datos**
2. **Servidor de autenticación**
3. **Servidor de aplicaciones**

Cada servidor requiere una configuración de hardware específica. La Plataforma proporcionará opciones de hardware básicas y recomendadas para garantizar la escalabilidad y la capacidad de gestionar un aumento del tráfico.

Requisitos de hardware recomendados:

1. **Servidor de base de datos:**

Recomendado: 64 GB de RAM, 1 TB de disco duro, sistema operativo Linux (Ubuntu 22.04 o Red Hat 8/9.3)

2. **Servidor de autenticación:**

Recomendado: 32 GB de RAM, 100 GB de disco duro, sistema operativo Linux (Ubuntu 22.04 o Red Hat 8/9.3)

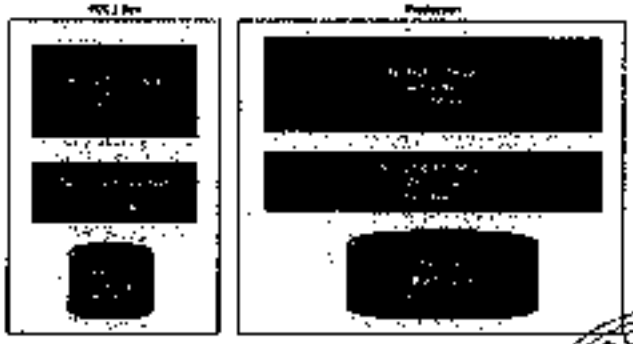
3. **Servidor de aplicaciones:**

Recomendado: 128 GB de RAM, 500 GB de disco duro, sistema operativo Linux (Ubuntu 22.04 o Red Hat 8)

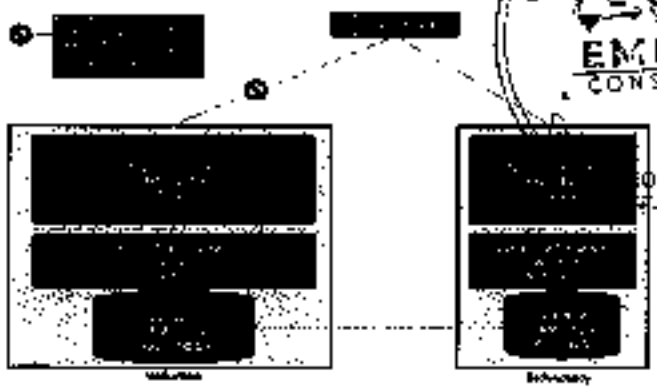
Modelos de infraestructura:

Al adherirse a estas especificaciones, el método de despliegue multihost on-premise garantizará un rendimiento, una escalabilidad y un control sólidos, adaptados para satisfacer las demandas de su infraestructura. A continuación encontrará ejemplos de los modelos POC, Producción, Redundancia y Recuperación ante desastres:

POC/Modelo de producción:

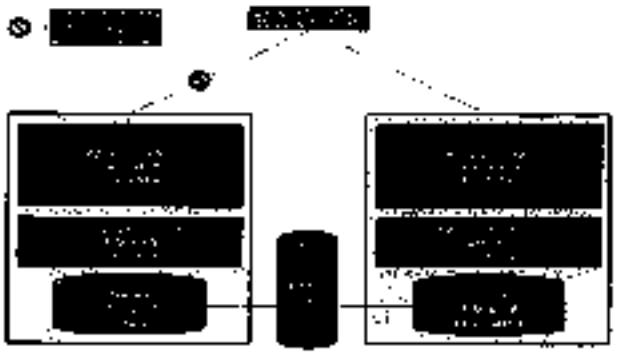


Modelo de redundancia:



CONSORCIO EMDOC
EMDOC
CONSORCIO

Modelo de recuperación en caso de catástrofe:



2.6. Proceso de actualización local para Docker

Proceso de actualización de Docker local

Objetivo:
Garantizar una actualización fluida de Docker con una interrupción mínima de los servicios.

Preparación:

1. **Haga una copia de seguridad de los datos esenciales:**
   Antes de la actualización, hay que hacer una copia de seguridad de todos los datos y configuraciones esenciales para garantizar que puedan restaurarse en caso necesario.
2. **Notificar a las partes interesadas:**
   Informe a todas las partes interesadas de la actualización programada, incluidos los plazos previstos y las posibles interrupciones del servicio.

Pre-Check:

1. **Confirme la versión actual de Docker:**
   Verifique la versión de Docker existente para comprender el alcance de la actualización.
2. **Revise los cambios de la nueva versión:**
   Evalúe las notas de la versión y los cambios en la nueva versión de Docker para anticipar cualquier impacto en las operaciones actuales.

Actualización:

1. **Detener contenedores en ejecución:**
   Detenga de forma segura todos los contenedores activos para evitar la corrupción de datos durante el proceso de actualización.

2. **Actualice Docker:**
   Ejecuta la actualización a la última versión de Docker, siguiendo los procedimientos adecuados para tu sistema operativo.
3. **Verifique la actualización:**
   Confirme que Docker se ha actualizado correctamente comprobando la versión y asegurándose de que todos los componentes funcionan como se espera.

Reiniciar y probar:

1. **Reiniciar Contenedores:**
   Inicia todos los contenedores detenidos previamente para reanudar el funcionamiento normal.
2. **Compruebe la funcionalidad de los servicios:**
   Compruebe que todos los servicios funcionan correctamente revisando los registros del contenedor y realizando pruebas básicas de funcionalidad.

Retroceso (si es necesario):

1. **Revertir versión Docker:**
   Si surge algún problema, vuelva a la versión anterior de Docker utilizando las copias de seguridad.
2. **Restaurar datos:**
   Si es necesario, restaura los datos de las copias de seguridad para asegurarte de que no se ha producido ninguna pérdida de datos.

Finaliza:

1. **Documente el proceso de actualización:**
   Registre todo el proceso de actualización, anotando los problemas encontrados y cómo se resolvieron.
2. **Notificar a las partes interesadas:**
   Comunique a las partes interesadas que se ha completado la actualización y facilite cualquier detalle o medida de seguimiento pertinente.

Despliegue azul-verde (local) - Estrategia de actualización

Blue-Green Deployment es una estrategia para lanzar nuevas versiones de software con un tiempo de inactividad y un riesgo mínimos. Requisito previo: Se utilizan dos entornos idénticos:

- **Entorno Azul:** La versión actual en vivo (por ejemplo, la versión 1.0.1 del servicio IAM) a la que acceden los usuarios.
- **Entorno verde:** La nueva versión (por ejemplo, la versión 1.0.2 del servicio IAM) que está lista pero aún no está en funcionamiento.

Pasos de actualización Ejemplo:

1. **Configuración actual:** La versión 1.0.1 está activa y atendiendo a los usuarios.
2. **Nueva versión desplegada:** La versión 1.0.2 está desplegada pero aún no sirve a los usuarios.
3. **Cambiar el tráfico:** Una vez que se confirma que la versión 1.0.2 funciona correctamente, se activa y los usuarios son redirigidos a ella.
4. **Monitor:** Si todo funciona según lo previsto, se elimina la versión antigua (1.0.1).
5. **Fallback:** Si hay problemas, el tráfico vuelve a la versión 1.0.1

Modelo de reserva:



2.7. Mantenimiento de la Plataforma

Visión general

El mantenimiento de la plataforma de Mobile ID en un entorno local es fundamental para garantizar la fiabilidad del sistema, la escalabilidad y un tiempo de inactividad mínimo. En esta sección se describen procedimientos estructurados que abarcan la redistribución de servicios, las actualizaciones de clústeres Kubernetes, el escalado automático de nodos de trabajadores y las copias de seguridad de bases de datos. Estos procesos están diseñados para mantener la eficiencia operativa al tiempo que se minimizan las interrupciones del servicio.

Redistribución de servicios

Los servicios de Mobile ID utilizan una estrategia de despliegue Blue-Green para garantizar transiciones de servicio fluidas con un tiempo de inactividad mínimo. Cada servicio mantiene dos configuraciones de implantación con distintas versiones de imagen almacenadas en un registro de contenedores interno. Para IAM, ConfigServer y WebUI, las configuraciones de implantación hacen referencia a diferentes versiones de imagen. Cualquier cambio en la configuración, los certificados, las imágenes base o la funcionalidad requiere la reconstrucción de la imagen más reciente utilizando el archivo Docker, enviándola al registro interno y desplegándola mediante un script de

redespliegue. Las actualizaciones se gestionan mediante modificaciones del archivo YAML. La misma estrategia de despliegue se aplica a los servicios CMS, UserManagement y Gateway para garantizar la coherencia y los despliegues controlados.

Actualizaciones del clúster Kubernetes

Para mantener la estabilidad y la seguridad de Kubernetes, el proceso de actualización del clúster sigue metodologías de actualización no disruptivas. Las actualizaciones pueden realizarse mediante herramientas nativas de Kubernetes, como kubectl, kubeadm o la automatización de Ansible. Estas actualizaciones garantizan que las versiones de Kubernetes permanezcan actualizadas sin afectar a las cargas de trabajo en ejecución. Los administradores pueden modificar los archivos de configuración para gestionar eficazmente los cambios de versión, manteniendo la estabilidad del clúster y el cumplimiento de las normas de seguridad.

Autoescalado del nodo de trabajo

El autoescalado se implementa para ajustar dinámicamente la asignación de recursos, garantizando la optimización de costes y el rendimiento del sistema. El servidor de métricas recopila datos de CPU y memoria en tiempo real para facilitar una supervisión eficaz. El Cluster Autoscaler añade automáticamente nodos trabajadores cuando los pods permanecen en estado pendiente debido a recursos insuficientes.

El autoescalado de pods ajusta dinámicamente el número de réplicas por microservicio en función de la CPU, la memoria o métricas personalizadas. El autoescalado horizontal de pods (HPA) garantiza que siempre haya disponible un mínimo de dos réplicas, al tiempo que aumenta la escala a medida que aumenta la demanda. Las políticas de escalado definen las tasas de adición y eliminación de pods, con ventanas de estabilización que garantizan ajustes suaves. El escalado automático se activa cuando la utilización de la CPU o la memoria supera el 75%, lo que evita la degradación del rendimiento.

Copia de seguridad y recuperación de bases de datos

Las estrategias de copia de seguridad de bases de datos se gestionan mediante scripts de automatización y herramientas de gestión de la configuración como Ansible o Terraform para garantizar la integridad de los datos y las capacidades de recuperación.

Protección contra el borrado: Se aplican medidas de protección contra el borrado para evitar el borrado accidental de la base de datos.

Configuración de instantáneas: Se toman instantáneas automáticas antes de finalizar la base de datos, lo que garantiza que las copias de seguridad sigan estando disponibles.

Retención de copias de seguridad: Las copias de seguridad se conservan durante siete días, con una ventana de copia de seguridad diaria que minimiza la posible pérdida de datos.

En caso de fallo, se puede crear una nueva instancia de base de datos a partir de la instantánea más reciente. Las actualizaciones de los registros DNS internos

garantizan una redirección sin problemas a la nueva instancia de base de datos. El proceso de restauración implica la identificación de la última instantánea, la recreación de la base de datos y la actualización de las configuraciones DNS para reflejar el nuevo punto final.

Siguiendo estos procedimientos de mantenimiento, la plataforma Mobile ID garantiza una alta disponibilidad, escalabilidad y una sólida protección de los datos. El enfoque estructurado del despliegue, las actualizaciones, el autoescalado y las copias de seguridad garantiza la continuidad operativa con un impacto mínimo en los usuarios finales. Estos procesos contribuyen a la fiabilidad de la plataforma, reduciendo el tiempo de inactividad y optimizando el rendimiento del sistema.

2.8. Análisis de interfaces y plan de pruebas para interfaces de comunicación

Análisis de interfaces y plan de pruebas para interfaces de comunicación

Reconocemos la necesidad de un análisis exhaustivo y un plan de pruebas para garantizar el éxito del ajuste y la integración de las interfaces de comunicación propuestas por el CCE. Nuestro enfoque está diseñado para proporcionar una evaluación exhaustiva de la arquitectura de interfaz, garantizando el cumplimiento, la interoperabilidad y el rendimiento, al tiempo que aborda los posibles desafíos durante la fase de implementación.

Enfoque del análisis de interfaces

Nuestra metodología de análisis de interfaces se centra en comprender los requisitos, evaluar la compatibilidad e identificar los posibles problemas de integración. Los pasos clave de nuestro enfoque incluyen:

1. **Recopilación de requisitos:**
    - Revisar las especificaciones propuestas para la interfaz de comunicación del JCE.
    - Identificar las dependencias técnicas y los puntos de contacto de integración.
    - Cumplir las normas del sector, como ISO/IEC 18013-5, y las directrices del NIST.
2. **Evaluación de interfaces:**
    - Evalúe la estructura de la interfaz (API RESTful, OIDC, SAML, colas de mensajes, etc.).
    - Analizar formatos de datos (JSON, XML, etc.) y protocolos de comunicación (HTTPS, NFC, BLE).

- Identificar posibles problemas de interoperabilidad con los sistemas existentes.

3 **Evaluación de la seguridad:**

- Realizar una evaluación de riesgos para identificar posibles vulnerabilidades en el proceso de intercambio de datos.
- Garantizar el cumplimiento de los requisitos de cifrado, autenticación y control de acceso.

4. **Consideraciones sobre escalabilidad y rendimiento:**

- Evalúe la capacidad de la interfaz para gestionar grandes volúmenes de solicitudes.
- Evalúe la latencia, los tiempos de respuesta y el consumo de recursos.

Plan de pruebas para el ajuste de la interfaz

Nuestro plan de pruebas propuesto esboza un enfoque estructurado para validar la integración de la interfaz, garantizando que la funcionalidad, la seguridad y el rendimiento cumplen las normas deseadas. El plan de pruebas incluye:

Objetivos de la prueba

- Validar la comunicación fluida entre sistemas.
- Garantizar la integridad y exactitud de los datos.
- Verificar el cumplimiento de los requisitos del JCE y de las normas aplicables.
- Identifique posibles cuellos de botella y optimice el rendimiento del sistema.

Fases de prueba

Pruebas unitarias:

- Aislar y probar los componentes individuales de la interfaz.
- Valide los puntos finales de la API, los formatos de solicitud/respuesta y la gestión de errores.

Pruebas de integración:

- Garantizar una interacción fluida entre nuestro sistema y la interfaz JCE.
- Verificar la corrección del mapeo y la transformación de datos.
- Pruebe la interoperabilidad con sistemas de terceros.

Pruebas funcionales:

- Evaluar los flujos de trabajo de extremo a extremo que implican el intercambio de datos entre sistemas.
- Confirmar la correcta gestión de la autenticación de usuarios, el control de acceso y los registros de transacciones.

Pruebas de seguridad:

- Realizar pruebas de penetración para identificar vulnerabilidades.
- Validar el cifrado de datos en tránsito y en reposo.
- Evaluar los mecanismos de autenticación y autorización.

Pruebas de rendimiento:

- Realizar pruebas de carga para medir la respuesta del sistema bajo cargas máximas.
- Realizar pruebas de estrés para determinar los límites del sistema.
- Evalúe los tiempos de respuesta y el rendimiento.

Pruebas de aceptación del usuario (UAT):

- Colaborar con las partes interesadas para validar la alineación de los procesos empresariales.
- Recoger opiniones para perfeccionar las interacciones de la interfaz.

Definición de escenarios de prueba

Nuestros escenarios de pruebas están diseñados para cubrir una amplia gama de casos de uso, lo que garantiza una validación exhaustiva de la funcionalidad de la interfaz:

Escenarios de intercambio de datos:

- Recuperación satisfactoria de datos de los sistemas JCE (por ejemplo, solicitudes de verificación de la identidad de los ciudadanos).
- Envío de datos a los sistemas JCE (por ejemplo, solicitudes de emisión de documentos).
- Tratamiento de entradas de datos incorrectas o incompletas.

Escenarios de gestión de errores:

- Mecanismos de tiempo de espera y reintento durante los fallos de comunicación.
- Uso incorrecto de la API (por ejemplo, tokens de autenticación no válidos).
- Tratamiento de casos extremos y entradas inesperadas.

Escenarios de seguridad:

- Intentos de acceso no autorizados.
- Gestión y expiración de sesiones.
- Cumplimiento del GDPR y otros requisitos normativos.

Escenarios de rendimiento:

- Pruebas con usuarios simultáneos accediendo al sistema.
- Medición de los tiempos de respuesta en transacciones de gran volumen.
- Evaluación del comportamiento del sistema durante la latencia de la red.

Entregables

Como parte de nuestra respuesta, proporcionaremos los siguientes entregables para apoyar el proceso de ajuste de la interfaz:

Informe exhaustivo de análisis de interfaces:

- Resumen de conclusiones y recomendaciones.
- Identificación de riesgos de integración y estrategias de mitigación.

Documento detallado del plan de pruebas:

- Plan de ejecución paso a paso para cada fase de las pruebas.
- Criterios de aceptación para una integración satisfactoria.

Informes de ejecución de pruebas:

- Resultados de los casos y escenarios de prueba realizados.
- Puntos de referencia de rendimiento y seguimiento de problemas.

Confiamos en que nuestro enfoque garantice un proceso de integración fluido y eficaz, manteniendo al mismo tiempo los más altos niveles de calidad, seguridad y rendimiento. Esperamos poder colaborar con JCE y ofrecerle más información durante la fase de implantación.

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo

Anexo

Apéndica 1- Visión general de la arquitectura de la plataforma

Diagrama de la plataforma de identificación móvil

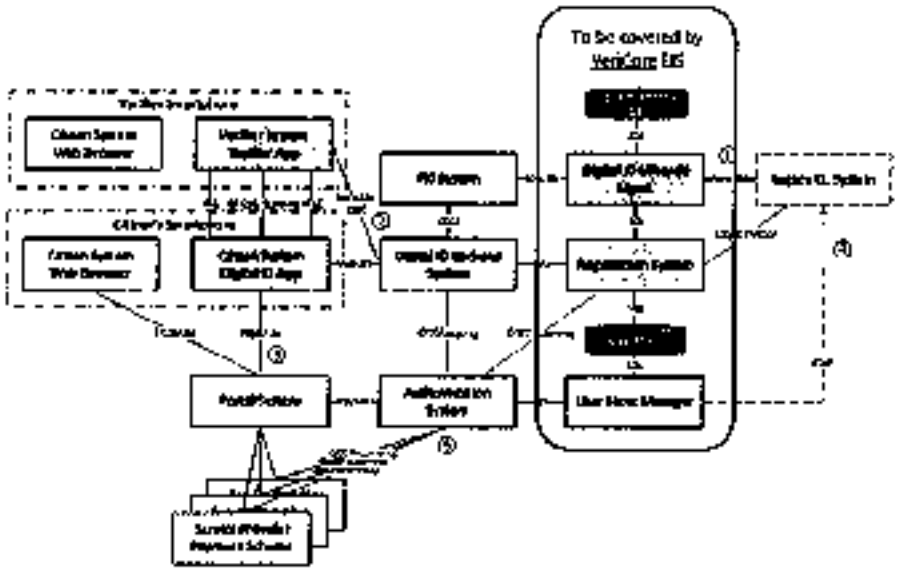
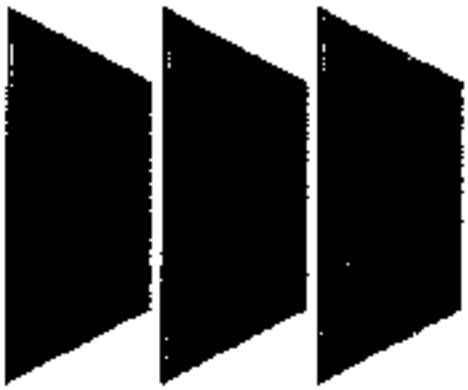
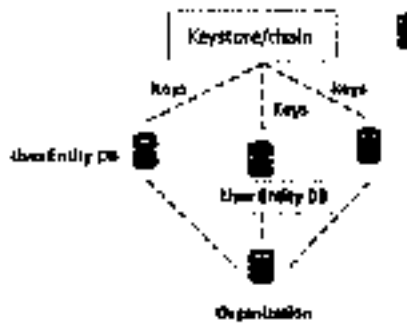


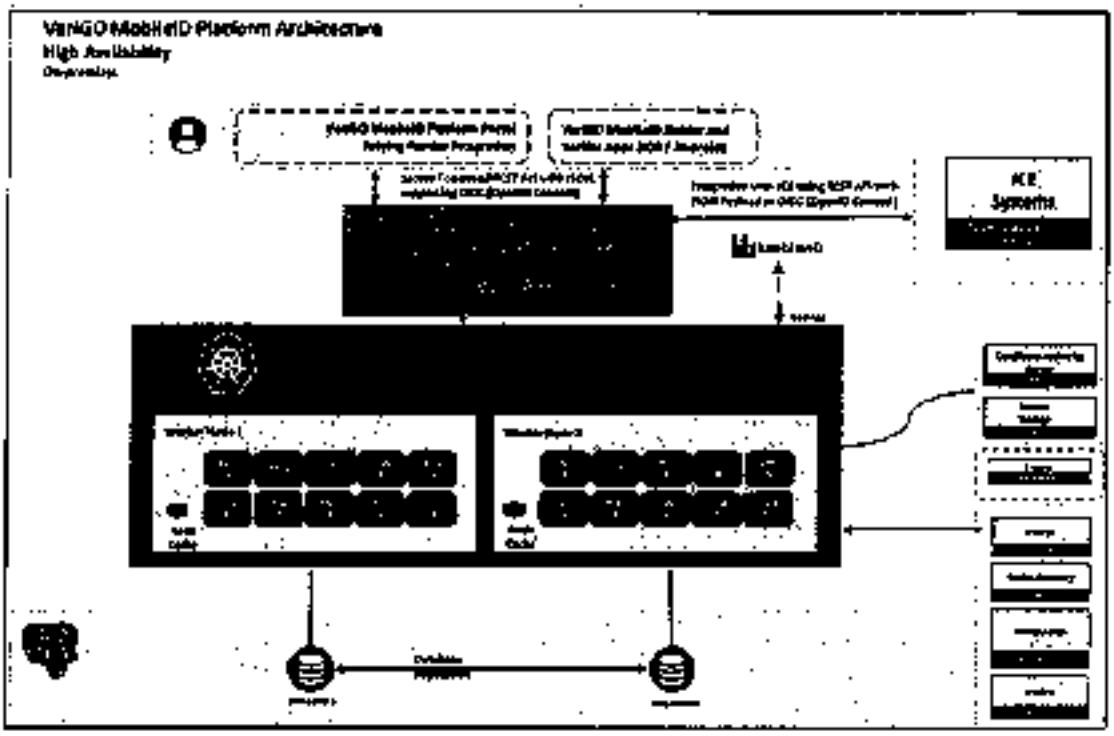
Fig. 1: mID Architecture – Component View

Plataforma ID Cartera Ilustración de credencial independiente dentro de la misma cartera.





Integración con el sistema heredado JCE



La plataforma se ajusta a las normas internacionales pertinentes:

- Certificación ISO/IEC 18013-5 y compatibilidad con ISO/IEC 18013-7 en permisos de conducir móviles y otros casos de uso de mDoc como certificaciones, diplomas, matriculación de vehículos, etc.
- Directrices de implantación del mID/mDL de la AAMVA
- Norma del W3C sobre credenciales verificables

Tecnologías utilizadas en la plataforma VeriGO MobileID

Normas	Acciones
Inquilino a bordo	Proceso de aprovisionamiento gestionado internamente
Microservicio Spring Boot	- OpenJDK 8/17 - Config-server- añadir o eliminar tenant - URI Endpoints- incluir identificador de inquilino

Base de datos (Compartida)	Postgres v15.1 - RLS (Row Level Separation) en la base de datos Todas las tablas con datos PII e de inquilinos contienen la columna de identificación del inquilino.
Protocolos	OIDC, SAML 2.0, OAuth2.0, LDAP-AD, SCIM 2.0
Credenciales	Credencial verificable, FIDO2, PUSH(Consentimiento), PKI, OTP
Infraestructura	En las instalaciones / AWS en la nube

- Auditorías de seguridad periódicas: Se llevarán a cabo auditorías de seguridad periódicas para identificar y abordar las vulnerabilidades.
- Cumplimiento de la normativa: El sistema cumplirá la normativa pertinente sobre protección de datos, como el GDPR, para garantizar la privacidad de los usuarios.

Apéndice 2 Ejemplo de caso de prueba

Los casos de prueba de la plataforma móvil de identificación proporcionados se utilizan actualmente en nuestros calendarios de pruebas para la plataforma en relación con el uso de la misma, las pruebas de regresión cuando se añaden nuevas funciones y cuando se desarrolla la documentación para su uso a nivel de usuario, agente y administración. Nuestro enfoque, tal y como se ha explicado anteriormente, se dirigirá hacia el éxito del despliegue, mantenimiento, seguridad y rendimiento de la plataforma con la colaboración del JCE.

A continuación se ofrece un ejemplo del formato y los casos de prueba actuales que se tendrán en cuenta durante la transferencia de conocimientos

Información de cabecera

- **Nombre/Título del proyecto**: Indique claramente el nombre de la licitación e del proyecto.
- **Número de referencia de la licitación**: Incluya el número de referencia para facilitar su identificación.
- **Versión del documento del caso de prueba**: Menciona la versión para gestionar las actualizaciones.
- **Fecha**: Especifique la fecha de presentación del caso de prueba,

- **Preparado por**: Identifique al agente o departamento que proporciona los casos de prueba.

Visión general

- **Objetivo**: Indicar el propósito de los casos de prueba, como validar entregables específicos, garantizar el cumplimiento de requisitos funcionales o confirmar especificaciones no funcionales.
- **Alcance**: Definir el alcance de las pruebas, incluidos los límites y las exclusiones.
- **Supuestos/Dependencias**: Enumere las suposiciones o dependencias que deben existir para que se ejecuten las pruebas.

Detalles del caso de prueba

El formato tabular es la forma más habitual y eficaz de presentar los casos de prueba:



Entorno de pruebas

- **Requisitos de hardware**: Mencione cualquier hardware específico necesario para las pruebas.
- **Requisitos de software**: Incluye sistemas operativos, herramientas o librerías necesarias para la ejecución
- **Requisitos de red/conectividad**: Especifique si se necesita Internet, protocolos específicos o configuraciones.

Entregables

- Una lista de los resultados esperados de la fase de pruebas, por ejemplo:
  - Informes de ejecución de casos de prueba.
  - Capturas de pantalla, registros u otras pruebas de validación.
  - Informes de defectos, si procede.

Criterios de aceptación

- Definir los criterios de aceptación de los casos de prueba o de los resultados de las pruebas.
- Especifique parámetros de rendimiento, porcentajes mínimos de aprobados o umbrales de cumplimiento.

Notas/Instrucciones

- Incluya notas o instrucciones especiales para los revisores.

Si sigue una norma específica (por ejemplo, ISO, ISTQB), menciónela.

CONSORCIO EMDOC
EMDOC CONSORCIO
Santo Domingo, R.D.

ÍTEM IV. VeriGo MobileID – Anexo Casos de Uso

PARA LA CONTRATACIÓN DE LA EMPRESA QUE SE ENCARGARÁ DE SUPLIR LOS EQUIPOS, MATERIALES Y SERVICIOS PARA LA IMPRESIÓN DE LA CÉDULA DE IDENTIDAD Y ELECTORAL (CIE) Y CÉDULA DE IDENTIDAD (CI)

CONSORCIO EMDOC
EMDOC
Santo Domingo, R.D.

178-2

EMDOC

CONTENIDO

1 Prueba de Vida 3
2 Privacidad 4
3 Apéndice - Casos de uso de la plataforma VeriGO MobileID 5
3.1. Casos prácticos 5

CONSORCIO EMDOC
EMDOC
Santo Domingo, RD

1 **Prueba de Vida**

La solución debe utilizar durante el proceso de emisión o activación de la identidad digital, el mecanismo de detección de liveness (prueba de vida), con el fin de evitar ataques de presentación.

Veridos acepta y cumple este requisito

VeriGO MobileID admite la activación del identificador móvil con detección de liveness y una comparación 1:1 del selfie generado por el ciudadano con el sistema de registro en el lado del servidor.

La tecnología de detección de ataques de presentación incluida en VeriGO MobileID está certificada según la norma ISO/IEC 30107.

En la secuencia siguiente se visualiza el proceso de detección de vida





CONSORCIO EMDOC
EMDOC
Santo Domingo R.D.

2 Privacidad

Las aplicaciones móviles deben tener la capacidad de compartir únicamente la información que el digitaltitular de la identidad desea compartir, en el momento de la verificación de la identidad.

Veridos acepta y cumple este requisito

Se trata de una función estándar de VeriGO MobileID para priorizar la privacidad y la comodidad del usuario. La minimización de datos definida por el usuario es un principio básico de la especificación ISO/IEC 18013-5.

Cuando se inicia el compromiso del dispositivo entre el titular y el verificador, se informa al titular de los atributos cuya verificación se solicita.

A continuación se ilustra un proceso de verificación típico configurable:



CONSORCIO EMDOC
EMDOC
Santo Domingo, R.D.

3 Apéndice - Casos de uso de la plataforma VeriGO MobileID

3.1. Casos prácticos

Usuario	Un tipo de actor (rol) que es el usuario final de la Plateforme VeriGO MobileID.
Administrador	Un tipo de actor (rol) cuya responsabilidad principal es interactuar con los usuarios finales y verificadores y proporcionar servicios relacionados con y/o gestionar el programa de la Plataforma VeriGO MobileID.
Verificador	Un tipo de actor (rol) cuya responsabilidad principal es consumir los datos de la Plataforma VeriGO MobileID para sus respectivos fines.

Caso de uso 1: descargar la aplicación VeriGO MobileID Platform de app store / google play
Historia de usuario Yo, como usuario, puedo descargar la aplicación VeriGO MobileID Platform desde la tienda de aplicaciones o google play.
Condición previa El usuario está en posesión de una credencial autorizada que residirá en el teléfono móvil. Las aplicaciones para titulares y verificadores de la plataforma VeriGO MobileID están disponibles públicamente en app store o google play store.
Post-condición La aplicación VeriGO MobileID Platform reside ahora en el smartphone, pero aún no está personalizada con la credencial del usuario.
Acciones del proceso de negocio El usuario visita la app store / google play store con su dispositivo compatible. El usuario descarga la aplicación VeriGO MobileID Platform en su smartphone. El usuario registra su cuenta y recibe instrucciones sobre cómo obtener su credencial digitalizada.

CONSORCIO EMDOC
EMDOC
Santo Domingo R.D.

Caso de uso 4: activar la plataforma VeriGO MobileID
Historia de usuario Como usuario quiero activar mi Plataforma VeriGO MobileID después de que haya sido aprobada.
Condición previa El usuario ha sido aprobado para una Plataforma VeriGO MobileID y ésta ha sido emitida.
Post-condición La plataforma VeriGO MobileID del usuario reside ahora en su smartphone.
Acciones del proceso de negocio El usuario recibe instrucciones que describen cómo cargar la identificación de la Plataforma VeriGO MobileID en su smartphone. El usuario adquiere la aplicación VeriGO MobileID Platform. Esto puede estar integrado en la plataforma móvil, en cuyo caso el usuario tendría que activar la funcionalidad de la Plataforma VeriGO MobileID. Esto puede activarse descargando e instalando una aplicación que resida en la tienda de aplicaciones de un proveedor. El usuario inicia la aplicación VeriGO MobileID Platform. El usuario autentica su identidad a través de la aplicación VeriGO MobileID Platform utilizando la credencial segura creada durante la inscripción. El usuario crea una nueva credencial para controlar el acceso a la Plataforma VeriGO MobileID. Las funciones de visualización y autenticación de la Plataforma VeriGO MobileID están activadas.

CONSORCIO EMDOC
EMDOC
Santo Domingo D.C.

Caso de uso 7: Verificación de la plataforma VeriGO MobileID - sin conexión

Historia de usuario

Yo, como usuario, quiero presentar mi Plataforma VeriGO MobileID para su verificación fuera de línea (recuperación del dispositivo).
Yo, como verificador, quiero verificar una plataforma VeriGO MobileID fuera de línea (recuperación del dispositivo).

Condición previa

El usuario puede presentar su plataforma VeriGO MobileID.
El usuario proporciona el permiso de autenticación para verificar su plataforma VeriGO MobileID.
El verificador dispone de un mecanismo para autenticar la plataforma VeriGO MobileID.

Post-condición

El verificador ha comprobado la autenticidad de la Plataforma VeriGO MobileID, incluida la identidad del titular de la Plataforma VeriGO MobileID.

Acciones del proceso de negocio

El usuario visita la app store / google play store con su dispositivo compatible.

El verificador solicita permiso para autenticar la Plataforma VeriGO MobileID.

El usuario concede al verificador permiso para autenticar la Plataforma VeriGO MobileID

Flujo de excepción: el usuario no concede al verificador permiso para autenticar la Plataforma VeriGO MobileID y el flujo del caso de uso finaliza.

El verificador utiliza un smartphone para comunicarse con la plataforma VeriGO MobileID.

El verificador comprueba la autenticidad de la plataforma VeriGO MobileID y los privilegios de conducción del usuario mediante el smartphone.

Flujo alternativo: si el verificador sospecha que la plataforma VeriGO MobileID no es auténtica, puede solicitar una tarjeta física o llamar a una central o línea directa para obtener información adicional que le ayude a verificar la autenticidad de la plataforma VeriGO MobileID.

Flujo de excepción: si la Plataforma VeriGO MobileID no puede verificarse, se rechaza y el flujo del caso de uso finaliza.

El verificador comprueba la identidad de la persona que presenta la Plataforma VeriGO MobileID.

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo R.D.

Flujo de excepción: si el verificador no puede comprobar que la persona que presenta la Plataforma VeriGO MobileID coincide con la credencial, ésta será rechazada y el flujo del caso de uso finalizará.

El permiso del verificador para acceder a la Plataforma VeriGO MobileID del usuario expira una vez finalizada la interacción.

CONSORCIO EMDOC
EMDOC
Santo Domingo R.D.

Caso 10: divulgación selectiva de datos
Historia de usuario Yo como usuario con proporcionar a un verificador acceso a información específica y privilegios asociados con mi Plataforma VeriGO MobileID. Como verificador, deseo ver y verificar información específica y privilegios asociados a la Plataforma VeriGO MobileID del usuario
Condición previa El usuario ha proporcionado permiso para acceder a información específica y privilegios asociados a su Plataforma VeriGO MobileID. El verificador dispone de un mecanismo para verificar la Plataforma VeriGO MobileID.
Post-condición El verificador ha verificado la información específica y/o los privilegios asociados a la Plataforma VeriGO MobileID.
Acciones del proceso de negocio El usuario visita la app store / google play store con su dispositivo compatible. El verificador solicita permiso para acceder a la Plataforma VeriGO MobileID y ver la información personal y los privilegios específicos asociados a la Plataforma VeriGO MobileID. El usuario concede al verificador permiso para ver los privilegios solicitados: Flujo de excepción: un usuario no concede al verificador permiso para ver los privilegios solicitados y el flujo del caso de uso finaliza. El verificador sólo visualiza la información y los privilegios que el usuario ha autorizado a ver, junto con una marca de tiempo que refleja la actualización en línea más reciente de estos privilegios. El permiso del verificador para ver los privilegios del usuario expira una vez finalizada la interacción.

CONSORCIO EMDOC
EMDOC
Santo Domingo, R.D.

Caso de uso 11: suministro de atributos de usuario de la aplicación VeriGO MobileID Platform a la aplicación VeriGO MobileID Platform
Historia de usuario Como usuario, deseo intercambiar información de la Plataforma VeriGO MobileID con otro usuario.
Condición previa Ambos usuarios tienen una plataforma VeriGO MobileID activa.
Post-condición Un usuario ha verificado a la Plataforma VeriGO MobileID de otro usuario. La actividad de intercambio de información se registra / graba.

CONSORCIO EMDOC
EMDOC
Santo Domingo, R.D.

Historia de usuario
Como usuario, quiero trasladar mi plataforma VeriGO MobileID de un smartphone a otro en una oficina gubernamental.
Como administrador quiero determinar la elegibilidad del usuario para transferir la Plataforma VeriGO MobileID.
Condición previa
El usuario está inscrito en el programa VeriGO MobileID Platform.
Post-condición
La Plataforma VeriGO MobileID del usuario se disocia del smartphone original.
La Plataforma VeriGO MobileID del usuario se asocia a un nuevo smartphone.
Acciones del proceso de negocio

El usuario visita la sede gubernamental e interactúa con un administrador de la Plataforma VeriGO MobileID.

El usuario solicita transferir el programa de la Plataforma VeriGO MobileID.

El administrador verifica la identidad del usuario.

El administrador determina si el usuario es elegible para transferir la Plataforma VeriGO MobileID.

Si cumple los requisitos, se proporciona al usuario un código de transferencia de un solo uso para que lo utilice en el nuevo teléfono inteligente.

El usuario descarga la plataforma VeriGO MobileID en el nuevo smartphone.

El usuario introduce el código de transferencia única en el nuevo smartphone.

Las credenciales de la plataforma VeriGO MobileID se transfieren al nuevo smartphone.

El usuario recibirá una confirmación de que la Plataforma VeriGO MobileID ha sido transferida a otro smartphone.

Se revocarán los permisos del smartphone original y ya no se podrá acceder a la Plataforma VeriGO MobileID del usuario. (esto es específico del cliente, ya que algunos clientes pueden desear permitir una Plataforma VeriGO MobileID en múltiples dispositivos).

CONSORCIO EMDOC
EMDOC
Santo Domingo R.D.

Caso de uso 13: cambiar de smartphone - online
Historia de usuario Como usuario quiero mover mi Plataforma VeriGO MobileID de un smartphone a otro de forma remota. Como administrador quiero determinar la elegibilidad del usuario para transferir la Plataforma VeriGO MobileID.
Condición previa El usuario está inscrito en el programa VeriGO MobileID Platform.
Post-condición La Plataforma VeriGO MobileID del usuario se disocia del smartphone original. La Plataforma VeriGO MobileID del usuario se asocia a un nuevo smartphone.
Acciones del proceso de negocio El usuario abre la aplicación de la Plataforma VeriGO MobileID o utiliza un navegador web para solicitar una transferencia de la Plataforma VeriGO MobileID a otro smartphone. Se verifica la identidad del usuario. El usuario confirma su intención de transferir la Plataforma VeriGO MobileID a otro smartphone. Se proporciona al usuario un código de transferencia de un solo uso que deberá utilizar en el nuevo teléfono inteligente. El usuario descarga la plataforma VeriGO MobileID en el nuevo smartphone. El usuario introduce el código de transferencia única en el nuevo smartphone. Las credenciales de la plataforma VeriGO MobileID se transfieren al nuevo smartphone. El usuario recibirá una confirmación de que la Plataforma VeriGO MobileID ha sido transferida a otro smartphone. Se revocarán los permisos en el smartphone original y ya no se podrá acceder a la plataforma VeriGO MobileID del usuario (esto es específico del cliente, ya que algunos clientes pueden desear permitir una plataforma VeriGO MobileID en varios dispositivos).

CONSORCIO EMDOC
EMDOC
Santo Domingo, R.D.

Caso de uso 14: Inscribirse como verificador - remoto en línea
Historia de usuario Como futuro verificador, deseo inscribirme en el programa como verificador en línea
Condición previa El verificador no está ya inscrito en el programa de la Plataforma VeriGO MobileID como verificador y posee un dispositivo compatible para la autenticación.
Post-condición El verificador es inscrito o rechazado del programa de la Plataforma VeriGO MobileID.
Acciones del proceso de negocio El verificador utiliza un navegador web para inscribirse en línea. El verificador solicita inscribirse en el programa de la Plataforma VeriGO MobileID como verificador. Se verifica la identidad del verificador. Se comprueba la elegibilidad del verificador para ser verificador del programa de la Plataforma VeriGO MobileID. El verificador revisa y acepta las cláusulas de exención de responsabilidad y los términos y condiciones. El verificador rellena y envía un formulario de inscripción de verificador de la Plataforma VeriGO MobileID. Se valida la información de inscripción y se completa la inscripción. El verificador recibe una credencial segura para autenticar la identidad.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

Historia de usuario
Yo, como futuro verificador, quiero inscribirme en el programa como verificador en una oficina gubernamental.
Condición previa
El verificador no está ya inscrito en el programa de la Plataforma VeriGO MobileID como verificador y posee un dispositivo compatible para verificador.
Post-condición
El verificador es inscrito o rechazado del programa de la Plataforma VeriGO MobileID.
Acciones del proceso de negocio

El verificador visita una oficina gubernamental.

El verificador solicita inscribirse en el programa de la Plataforma VeriGO MobileID como verificador.

Se verifica la identidad del verificador.

Se comprueba la elegibilidad del verificador para ser verificador del programa de la Plataforma VeriGO MobileID.

El verificador revisa y acepta las cláusulas de exención de responsabilidad y los términos y condiciones.

El verificador rellena y envía un formulario de inscripción de verificador de la Plataforma VeriGO MobileID.

Se valida la información de inscripción y se completa la inscripción.

El verificador recibe una credencial segura para autenticar la identidad.

CONSORCIO EMDOC
EMDOC
Santo Domingo, R.D.

178-15

EMDOC

Caso de uso 16. verificación visual / manual de la plataforma VeriGO MobileID

Historia de usuario
Yo, como verificador, quiero acceder y validar la autenticidad de la Plataforma VeriGO MobileID en ausencia de dispositivos de autenticación digital utilizando la inspección visual y manual y los medios tradicionales de verificación.

Nota: los aspectos de cumplimiento material no se reproducen en la plataforma VeriGO MobileID (por ejemplo, permitir a un agente de la ley en una zona rural sin acceso a la red inalámbrica validar una plataforma VeriGO MobileID llamando al despacho central y verificando la identidad. el privilegio de conducción, la descripción y las características de seguridad de una plataforma VeriGO MobileID).

Condición previa
El usuario puede proporcionar al verificador acceso a la plataforma VeriGO MobileID.

Post-condición
El verificador ha comprobado la autenticidad de la Plataforma VeriGO MobileID o la identidad del usuario.

Acciones del proceso de negocio

El verificador solicita permiso para autenticar la Plataforma VeriGO MobileID.

El usuario concede al verificador permiso para autenticar la Plataforma VeriGO MobileID

> Flujo de excepción: el usuario no concede al verificador permiso para autenticar la Plataforma VeriGO MobileID y el flujo del caso de uso finaliza.

El verificador examina la información mostrada en la plataforma VeriGO MobileID.

El verificador comprueba la autenticidad de la plataforma VeriGO MobileID y los privilegios de conducción del usuario.

> Flujo alternativo: si el verificador sospecha que la plataforma VeriGO MobileID no es auténtica, puede solicitar una tarjeta física o llamar a una central o línea directa para obtener información adicional que le ayude a verificar la autenticidad de la plataforma VeriGO MobileID.

Si la Plataforma VeriGO MobileID sigue sin poder verificarse, se rechaza y el flujo del caso de uso finaliza.

El verificador comprueba la identidad de la persona que presenta la Plataforma VeriGO MobileID.

CONSORCIO EMDOC EMDOC TECNOLOGIA SANTO DOMINGO, D.N.

178-16

EMDOC

Caso práctico 17: funcionalidad de firma
Historia de usuario Como usuario, quiero firmar digitalmente un documento electrónico después de autenticar y cargar correctamente el documento.
Condición previa El usuario se ha registrado en el servicio de firma, se ha generado un par de claves y un certificado de firma y se ha emitido al usuario. El usuario tiene una Plataforma VeriGO MobileID activa.
Post-condición El documento del usuario ha sido firmado digitalmente.
Acciones del proceso de negocio El usuario solicita acceso al servicio de firma electronica El servicio de firma solicita la autenticación del usuario mediante la aplicación móvil. El usuario se autentica utilizando una autenticación fuerte. El usuario carga el documento. El servicio de firma solicita una confirmación del usuario en la aplicación móvil. El usuario solicita la firma. El servidor de firma realiza la firma. El usuario descarga el documento firmado. El usuario se desconecta.

CONSORCIO EMDOC
EMDOC
Santo Domingo, R.D.

178-17

EMDOC

Historia de usuario
Yo, como usuario, puedo solicitar el acceso a una aplicación web publicada por un proveedor de servicios.
Condición previa
El usuario ha sido registrado por el sistema de registro en el almacén de usuarios del sistema de autenticación.

El proveedor de servicios se ha registrado y configurado en el sistema de autenticación.
Post-condición
El usuario ha recibido acceso a la aplicación web del proveedor de servicios solicitado.
Acciones del proceso de negocio

El usuario inicia el navegador web.

El usuario introduce el enlace del sistema del portal.

El sistema de portales ofrece acceso a aplicaciones web de varios proveedores de servicios.

El usuario selecciona el enlace al proveedor de servicios deseado.

La aplicación web del proveedor de servicios solicita una autenticación de acuerdo con la loa requerida.

La aplicación web redirige el navegador web del usuario al sistema de autenticación.

El sistema de autenticación muestra la página de inicio de sesión.

El usuario responde al inicio de sesión solicitado presentando su credencial, token, etc.

El servidor de autenticación autentica al usuario mediante sus datos en el almacén de usuarios.

El servidor de autenticación redirige al usuario a la aplicación web del proveedor de servicios.

La aplicación web del proveedor de servicios solicita el token de acceso al servidor de autenticación.

El servidor de autenticación responde con el token de acceso.

La aplicación web verifica la autenticidad del token de acceso.

La aplicación web del proveedor de servicios concede acceso a la aplicación web.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

Caso 19: acceso a la aplicación
Historia de usuario Como usuario, quiero proteger y abrir mi aplicación VeriGO MobileID Platform. Para ello se puede utilizar un código de 4-6 dígitos o la biometría integrada en el smartphone (identificación facial, identificación táctil).
Condición previa La aplicación VeriGO MobileID Platform está bloqueada y no se puede acceder a ella hasta que se pida al usuario que introduzca su código de acceso o proporcione sus datos biométricos.
Post-condición La aplicación VeriGO MobileID Platform está desbloqueada y puede utilizarse.
Acciones del proceso de negocio El usuario visita la app store / google play store con su dispositivo compatible. Durante el registro, se pedirá al usuario que añada una contraseña para proteger la aplicación. Durante el registro, también se puede pedir al usuario que utilice datos biométricos para proteger la aplicación. El usuario introducirá la contraseña o los datos biométricos para abrir la aplicación VeriGO MobileID Platform. Si el código de acceso o los datos biométricos son correctos, la aplicación se abrirá y estará lista para su uso. El usuario también puede optar por solicitar la introducción del código de acceso o los datos biométricos antes de iniciar la función de "entrega" de la aplicación VeriGO MobileID Platform para comenzar una transacción de identidad.

CONSORCIO EMDOC
EMDOC
Santo Domingo, R.D.

Caso práctico 20: suministro de atributos de usuario - servidor de autenticación

Historia de usuario

Yo, como aplicación web proveedora de servicios, puedo obtener atributos probados del usuario que solicita acceso a mis servicios.

Condición previa

El usuario ha sido registrado por el sistema de registro en el almacén de usuarios del sistema de autenticación.

El proveedor de servicios se ha registrado y configurado en el sistema de autenticación.

El usuario ha iniciado sesión en el sistema del portal.

Post-condición

La aplicación web del proveedor de servicios ha recibido los atributos de usuario solicitados.

La aplicación web del proveedor de servicios ha concedido acceso a sus servicios.

Acciones del proceso de negocio

El usuario selecciona el enlace al proveedor de servicios deseado.

La aplicación web del proveedor de servicios solicita un conjunto de atributos de usuario.

La aplicación web redirige el navegador web del usuario al sistema de autenticación.

El servidor de autenticación solicita el consentimiento del usuario para transmitir los atributos solicitados.

El servidor de autenticación redirige el navegador web del usuario a la aplicación web del proveedor de servicios.

La aplicación web del proveedor de servicios solicita el token de acceso al servidor de autenticación.

El servidor de autenticación responde con un token de acceso que incluye los atributos del usuario.

La aplicación web verifica la autenticidad del token de acceso.

La aplicación web proveedora de servicios concede acceso al servicio de aplicación web solicitado.

Historia de usuario
Yo, como administrador, pretendo enviar mensajes y notificaciones a un grupo de usuarios en función de un criterio definido.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

Caso de uso 22: solicitar productos y servicios adicionales
Historia de usuario Como usuario, deseo solicitar productos y servicios adicionales al organismo emisor. El caso lo inicia el usuario en línea.
Condición previa El usuario tiene una Plataforma VeriGO MobileID y un smartphone activos.
Post-condición La solicitud del usuario de productos y servicios adicionales se rechaza o se acepta.
Acciones del proceso de negocio El usuario utiliza la aplicación móvil VeriGO MobileID Platform. El usuario solicita productos y servicios adicionales. Se verifica la identidad del usuario. Se comprueba si el usuario cumple los requisitos para realizar la solicitud. El usuario revisa y acepta los descargos de responsabilidad, términos y condiciones, si los hubiera. El usuario rellena y envía cualquier información requerida, incluido el pago correspondiente, relacionada con los productos/servicios solicitados. Se valida la solicitud y se inicia el proceso de cumplimiento. El usuario recibe una confirmación de aceptación de la solicitud.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

178.22

EMDOC
CONSORCIO

COMPONENTES KIT PERIFERICOS

PARA LA CONTRATACIÓN DE LA EMPRESA QUE SE ENCARGARÁ DE SUPLIR LOS EQUIPOS, MATERIALES Y SERVICIOS PARA LA IMPRESIÓN DE LA CÉDULA DE IDENTIDAD Y ELECTORAL (CIE) Y CÉDULA DE IDENTIDAD (CI)

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

iQtek Mühlbauer High Tech International GSI ULTRATECH VIVERIDOS

EMDOC
CONSORCIO
179

COMPONENTES PARA LAS ESPECIFICACIONES DE KIT DE PERIFÉRICOS

El Consorcio EMDOC oferta un kit (conjunto completo) de periféricos con características similares o superiores. A continuación, brindamos un desglose detallado y unitario por cada uno de los periféricos que conforman el kit. El Consorcio EMDOC se compromete a suministrar dichos periféricos en un período de treinta (30) días calendario después de la solicitud de la JCE. Los precios podrán ser ajustados anualmente de acuerdo con la inflación. La JCE tiene la decisión de comprarlos o no.

V.1. Escáner:

Los escáneres cumplen con las siguientes especificaciones técnicas o superiores:

ITEM	REQUERIMIENTO
Marca:	Canon
Modelo:	SCANNER LIDE 300
Tipo:	Escáner móvil personal.
Alimentación de documentos:	Automática o manual.
Escala de grises:	Entrada de 16 bits -> salida de 8 bits
Color	Entrada de 48 bits -> salida de 48/24 bits
Fuente de luz:	LED RGB.
Modos de operación:	Color, escala de grises, blanco y negro.
Resolución óptica:	600 ppp.
Resolución de salida:	150/200/300/400/600/1200 ppp
Velocidades de escaneo:	(color) (Reflectante) 14,8 ms/línea (2400 ppp) 6,6 ms/línea (1200 ppp) 3,8 ms/línea (600 ppp) 2,2 ms/línea (300 ppp)3 (escala de grises, blanco y negro) (reflectante) 4,3 ms/línea (2400 ppp) 2,2 ms/línea (1200 ppp) 1,3 ms/línea (600 ppp) 2,2 ms/línea (300 ppp)



Interfaz:	USB 3.0 de alta velocidad
Otras características:	Detección automática de color.
	Detección automática de tamaño de página.
	Configuración automática de resolución.
	Suavizamiento de fondo.
	Corrección de desviación.
	Énfasis de borde.
	Reducción del efecto muaré.
	Corrección de fotografía.
	Escaneo previo.
	Eliminación de fondo/prevención de sangrado.
	Recorte del sombreado.
	Omisión de página en blanco.
	Mejoramiento de texto.
	Reconocimiento de la orientación del texto.
	Software incluido para Windows: Controladores WIA/TWAIN.
	Sistemas operativos compatibles: Windows 10, Windows 11.
No. de Serie de Muestra:	**KPEF39950**

V2. Lector de Firmas

Los lectores de firmas cumplen con las siguientes especificaciones técnicas o superiores:

ITEM	REQUERIMIENTO
Marca:	TOPAZ
Modelo:	SigLiTE LCD 4x3
Dimensiones del producto (aproximadas, similar o superior):	180 × 160 × 52 mm (7.1 × 6.3 × 2.0 pulgadas)
Interface de comunicación:	USB.
Tipo de resolución	F-STN, de alto contraste
Tamaño de pantalla:	+- 4.5".
Resolución nativa (aproximada, similar o superior):	Resolución nativa 240 × 128 píxeles
Niveles de presión del lápiz:	512/1024
Resolución del sensor:	2540 líneas por pulgada
Precisión de coordenadas:	± 0,5 mm (centro).
Bolígrafo sin pilas:	Si.
Bolígrafo inalámbrico:	Si.
Velocidad de transmisión (aproximada, similar o superior):	200 puntos por segundo (no interpolados)
No. de Serie de Muestra:	**750BHR24H6955**

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

V.3 Lector de huellas

Los lectores de huellas, son compatibles con NEUROtechnology toda vez que la JCE dispone de sistemas y software que usan esta tecnología y cumplen con las siguientes especificaciones técnicas o superiores:

ITEM	REQUERIMIENTO
Marca:	Integrated Biometrics
Modelo:	Kojak PL KP210DA
Tamaño de la ventana de escaneado de huellas dactilares:	Aproximado de 86 mm x 84mm
Área de escaneo óptico (aproximada, similar o superior):	81,2 mm x 76,3 mm / 3,2" x 3,0"
Resolución de la imagen (aproximada, similar o superior):	1600 x 1500 píxeles, 500 dpi.
Profundidad de bit	8 bit, 256 niveles de gris.
Tamaño del archivo Raw de la imagen de la huella dactilar comprimido en WSQ aprox.	2,5 MB aproximadas, similar o superior 0,4.
Interfaz (aproximada, similar o superior):	USB 2.0 de alta velocidad con cable USB estándar de alrededor de 1,8 metros
Fuente de luz diodos emisores de luz:	(LED) infrarroja.
Fuente de alimentación:	4.40V a 5.25V; 4.4 vía USB;
Indicar certificaciones:	• Certificaciones de Imagen/FBI • FBI Appendix F, FAP 60Certificaciones USB • USB-IF USB.ORG • Conformidad FCC/CE • FCC Parte 15 (por ANSI C63.4: 2014) Clase B, CSA ICES-003 • Clase B, CE Emisiones: EN 55022:2010 Class B, CE Immunity • EN 55024:2010/A1:2001/A2:2003, IEC 61000-4-2 • Descarga de Aire/Descarga de Contacto • En conformidad con IEC 61000-4-2 • Seguridad del Equipo

	• IEC 62368-1 • Material Peligroso • RoHS Directiva 2002/95/EC, TSCA, Proposición 65, Prohibición Canadá • Test de Vibración • IEC 60068-2-64 • Certificaciones • Formatos de salida de plantillas de huellas dactilares • ISO_19794_2_2005/2011, • ISO_19794_4_2005/2011 • ANSI_INCITS_378_2004/ANSI_INCITS_381_2004 • 00 PPI rollos y planos de soporte de captura de huellas dactilares • ISO 9001:2015 • ISO 30107-3 • MOSIP
No. de Serie de Muestra:	**KJ210DA-11700088-E00K**

v.4. Impresora de Punto de Venta:

Las impresoras de puntos de ventas cumplen con las siguientes especificaciones técnicas o superiores:

ITEM	REQUERIMIENTO
Marca:	Epson
Modelo:	TM-T20III
Ancho:	5,51"
Alto:	7,83"
Largo	5,75"
Calidad de impresión:	Alta resolución
Dimensiones (aproximadas, similar o superior):	5,51" x 7,83" x 5,75"
Cantidad de puertos USB: 1	1
Largo del cable (aproximado, similar o superior):	1.8
Compatible con :	Windows
Tipo de inyección:	Térmica
Color:	Negro

CONSORCIO EMDOC Santo Domingo, RD

Conectividad/conexión:	USB
Formato de papel:	80 mm: diámetro de 79,5 ± 0,5 (ancho) x 83 mm (3,13" ± 0,02" x 3,27") 58 mm: diámetro de 57,5 ± 0,5 (ancho) x 83 mm (2,26" ± 0,02" x 3,27")
Cantidad de bandejas:	1
Entrada:	USB
Velocidad de la impresión a blanco y negro (aproximada, similar o superior):	Velocidad de impresión de hasta 250 mm/s.
Tipo de impresión:	Térmica Monocromática
Número de serie de muestra:	**X7AU053031**

v.5. Lector de huella digital persona:

Los lectores de huellas digital persona, cumplen con las siguientes especificaciones técnicas o superiores:

ITEM	REQUERIMIENTO
Marca	Integrated Biometrics
Modelo	COLUMBO
Voltaje de suministro:	USB Nivel de Voltaje USB, 4.4V a 5.25V
Corriente de alimentación: escaneo (aproximada, similar o superior)	< 100 mA (típico).
Corriente de alimentación: en reposo (aproximada, similar o superior)	120 mA (típico)
Corriente de alimentación: modo suspensión (aproximada, similar o superior)	< 0,5 mA máximo
Inmunidad: (ESD, por sus siglas en inglés)	Contra descarga electroestática Descarga de Aire/Descarga de Contacto • En conformidad con IEC 61000-4-2 • >15 kV, montado en la caja.
Temperatura de operación:	• -10°C ~ +55°C / 14°F ~ 131°F
Humedad de almacenamiento:	• 20~95% RH < 40°C / 104°F (sin condensación)

CONSORCIO EMDOC Santo Domingo, RD

Información escaneada:	256 rango dinámico en escala de grises
Normas que cumple:	• Conformidad FCC/CE • FCC Parte 15 (por ANSI C63.4: 2014) Clase B, CSA ICES-003 • Clase B, CE Emisiones: EN 55022:2010 Class B, CE Immunity • EN 55024:2010/A1:2001/A2:2003, IEC 61000-4-2 • Descarga de Aire/Descarga de Contacto • En conformidad con IEC 61000-4-2 • Seguridad del Equipo • IEC 60950-1 • Material Peligroso • RoHS Directiva 2002/95/EC • Test de Vibración • Per Mil-STD-810F (Método 514.5), Categoría 24, Flg.514.5C-17"
Peso (aproximado, similar o inferior):	25 gramos / 0.06 lbs
Interfaz:	Dispositivo USB 2.0 de velocidad máxima, de alta potencia
No. de Serie de Muestra:	**CD110CA-12600271-000K**

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

v.6. Cámara

Las cámaras, cumplen con las siguientes especificaciones técnicas o superiores:

ITEM	REQUERIMIENTO
Marca	Canon
Modelo	EOS Rebel T100
Sensor:	CMOS.
Tecnologías:	IEEE 802.11b/g/n
Sistema:	• 9 puntos • Todos los puntos AF son compatibles con f/5.6 • AF tipo cruz con punto AF central (1) Enfoque automático • AF foto a foto • Servo AF AI predictivo • Enfoque AF con IA • Cambia automáticamente entre AF foto a foto y AF AI Servo
Visor óptico:	Visor óptico con una cobertura del visor de aproximadamente 95% (aproximado, similar o superior)
Alta definición real (Full HD) de	[Full HD]: 1920 x 1080 (30 fps/24 fps): 340 MB/min.
Balance automático de blancos	Balance automático de blancos con "Prioridad de blancos".
Puerto USB	Terminal de alta velocidad USB
Característica de autoenfoque:	• Enfoque automático 1. AF foto a foto 2. Servo AF AI predictivo 3. Enfoque AF con IA 4. Cambia automáticamente entre AF foto a foto y AF AI Servo. • Enfoque manual
Filtros	Enfoque Suave, Granulado Blanco/Negro, Efecto miniatura, Ojo de Pez y Cámara de Juguete
No. de Serie de Muestra:	**762072008002**

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

V 7 Lector RFID

Los lectores RFID cumplen con las siguientes especificaciones técnicas o superiores:

ITEM	REQUERIMIENTO
Marca:	VOTTAN
Modelo:	DS-K1F100
Dimensiones del producto (aproximadas, similar o superior):	110.5 mm×70 mm×11.5 mm
Interface de comunicación:	USB.
Frecuencia de lectura	13.56MHz
Protocolo	Norma ISO 14443 Tipo A/B y Norma ISO 7816
Temperatura de trabajo	20°C a 65 °C (4° F a 149°
Peso	87.6g
Cumplimiento	ICAO 9303 con interoperabilidad OACI DOC 9303, ISO18013, PA, AA, BAC, EAC , SAC.
No. de Serie de Muestra:	**N/A**



EMDOC
CONSORCIO

SECCIÓN ITEM VI. PARTE B.
ESPECIFICACIONES TÉCNICAS DEL MANTENIMIENTO

PARA LA CONTRATACIÓN DE LA EMPRESA QUE SE ENCARGARÁ DE SUPLIR LOS EQUIPOS, MATERIALES Y SERVICIOS PARA LA IMPRESIÓN DE LA CÉDULA DE IDENTIDAD Y ELECTORAL (CIE) Y CÉDULA DE IDENTIDAD (CI)

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

Contenido

1. *ESPECIFICACIONES TÉCNICAS DEL MANTENIMIENTO* 3

1.2. Tiempo de Solución 3

1.3. VI.2 Nivel de Servicio (SLA) 3

1.3.1. VI.2.1 Clasificación del nivel de servicio (SLA) 4

1.3.1.1. VI.2.1.1 Primer Nivel de Soporte (Hot Line o Línea Directa JCE) 4

1.3.1.2. VI.2.1.2 Segundo Nivel de Soporte (Especialista JCE) 4

1.3.1.3. VI.2.1.3 Tercer Nivel de Soporte (Soporte en-sitio) 4

1.3.1.4. VI.2.1.4 Prioridades de incidentes 5

VI.2.2 Definición de nivel de servicio en período de garantía para el proveedor 6

VI.2.2.1 Nivel de servicio para oficinas en Santo Domingo 6

1.4. VI.2.2.2 Niveles de servicios para oficinas en República Dominicana 7

1.4.1. VI.2.2.2.1 Tiempo de apoyo en sitio - Oficinas De República Dominicana 7

1.4.2. VI.2.2.3 Nivel de servicio para las oficinas de los Estados Unidos de América y resto del mundo. 8

2. *PLAN DE SOPORTE Y MANTENIMIENTO* 9

2.1. Mantenimiento Preventivo de Hardware y Software 9

2.1.1. Actividades del Mantenimiento Preventivo 9

2.2. Informe técnico del mantenimiento preventivo 11

2.3. Informe Ejecutivo periódico de mantenimiento preventivo 12

2.4. Mano de obra, insumos, transporte, otros para la prestación del mantenimiento preventivo 12

3. *MANTENIMIENTO CORRECTIVO DE HARDWARE Y SOFTWARE* 12

3.1. Actividades del mantenimiento correctivo 12

3.1.1. Modalidad para el mantenimiento correctivo 12

3.1.2. Informe Técnico Individual de mantenimiento correctivo por incidente, problema, error o falla 14

3.1.3. Informe Ejecutivo Periódico de mantenimiento correctivo 15

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

EMDOC CONSORCIO

1. ESPECIFICACIONES TÉCNICAS DEL MANTENIMIENTO

1.1. VI.1 Especificaciones técnicas del Mantenimiento

El Consorcio EMDOC brindará un soporte preventivo y correctivo durante toda la etapa del contrato, incluyendo a todas las impresoras, la PKI, la tarjeta digital y soluciones de software implementadas para integración de APIS de las impresoras con el actual sistema de identidad de la JCE, con disponibilidad de operación y mantenimiento del 99.95%, durante horas de producción, excepto por razones atribuibles a la JCE. El oferente.

El Consorcio EMDOC dispondrá de un centro regional de mantenimiento y reparación en República Dominicana, otro en USA y otro en Europa, y deberá tener en stock de inventario para reparaciones, como mínimo un 3% de inventario de suministro de las máquinas de personalización.

Para dar un correcto mantenimiento a la JCE, tanto en los centros de impresión en República Dominicana, USA y resto del mundo, el Consorcio EMDOC deberá proponer un equipo de mantenimiento, con experiencia comprobada para dar el mantenimiento. Para el mantenimiento a la PKI, se brindará soporte con personal de experiencia comprobada del Consorcio EMDOC.

El mantenimiento de las impresoras de tarjetas, al ser un elemento clave, debe ser ofrecido y operado por el personal técnico certificado por el fabricante de las impresoras tanto en sitio como de forma remota.El nivel de calidad del servicio se medirá mediante el SLA (Service Level Agreement).

1.2. Tiempo de Solución

El tiempo de solución de los incidentes reportados serán desde el momento en que sea notificado al **Consorcio EMDOC**, hasta el momento en que sean resueltos de la siguiente manera:

El alcance debe ser a nivel nacional e internacional, sin importar el volumen de impresión del centro.

1.3. VI.2 Nivel de Servicio (SLA)

El Consorcio EMDOC, brindará dos niveles de servicio:

1- Un nivel de servicio en garantía, que será brindado durante el primer año de servicio desde la instalación de los equipos de impresión, el PKI o la tarjeta digital, donde el proveedor tendrá que ir en sitio, a las oficinas de la JCE tanto a nivel nacional o internacional, dando soporte a nivel 3, es decir, es la JCE quien registra

la incidencia de los funcionarios (nivel 2), resuelve o escala a los técnicos de la JCE para que resuelvan la incidencia (nivel 2) y si no se resuelve con los técnicos de JCE, se re-escala al proveedor donde tendrá que ir a las oficinas en sitio (nivel 3) o podrá resolver de forma remota (si fuera posible).

2- Un nivel de servicio de mantenimiento (no en garantía) en la sede central de la JCE (para equipos de impresión en Rep. Dominicana o en el centro designado por la JCE en Nueva York o Madrid). Para PKI y tarjeta digital tendrá que ir al sitio central de la JCE o de forma remota.

1.3.1. VI.2.1 Clasificación del nivel de servicio (SLA)

1.3.1.1. VI.2.1.1 Primer Nivel de Soporte (Hot Line o Línea Directa JCE)

Cada tipo de incidente, que está relacionado con el equipo, debe ser informado a un sistema de boleta de servicio técnico o al servicio de atención en el centro de servicio central de la JCE en República Dominicana. El operador de la mesa de la JCE recoge la mayor cantidad posible de información sobre el incidente y brinda asistencia directa por medio de teléfono.

El formato de comunicación elegido para este nivel de soporte será:

- Email
- Teléfono

Este nivel de soporte será ofrecido por la JCE.

1.3.1.2. VI.2.1.2 Segundo Nivel de Soporte (Especialista JCE)

El soporte de segundo nivel será provisto por un técnico de JCE con un conocimiento más completo y especializado en los componentes del sistema.

El técnico apoyará al iniciador ya sea por teléfono o por acceso remoto. En el caso de que el incidente no se pueda resolver, el técnico especializado activa el soporte de tercer nivel en el sitio.

Este nivel de soporte será ofrecido por la JCE.

1.3.1.3. VI.2.1.3 Tercer Nivel de Soporte (Soporte en-sitio)

Este nivel de soporte será ofrecido por el Consorcio EMDOC, en caso de ser adjudicado por la JCE.

En caso de que un incidente no pueda resolverse por medio del soporte de segundo nivel, JCE abrirá un ticket de incidencia en el sistema de ticketing de JCE donde reportará

la incidencia al Consorcio EMDOC. Un experto especializado del Consorcio EMDOC debe de estudiar la incidencia, ponerse en contacto con JCE y organizar como resolver la incidencia, si de forma remota o yendo al sitio.

1.3.1.4. Vt.2.1.4 Prioridades de incidentes

Nivel de Prioridad	Impacto/Métricos		Descripción
	Componentes Centrales (PKI, Tarjeta de identidad digital)	Componentes Descentralizados (Impresoras, etc.)	
Critica	La capacidad de salida de todo el sistema se ve afectada y se reduce a 0%.	La capacidad de salida del sistema local se ve afectada y se reduce a 0%	Un error en un elemento central (hardware o software del centro de datos) que detiene por completo la capacidad de realizar un procesamiento de extremo a extremo o en una sede o consulado
Alta	La capacidad de salida del sistema se ve afectada y se reduce en >50%	La capacidad de salida del sistema local se ve afectada y se reduce en >50%	Una falla en un elemento de los sistemas instalados que limita o reduce significativamente la capacidad de realizar el procesamiento de documentos de extremo a extremo.
Mediana	La capacidad de salida del sistema se ve afectada y se reduce en >10%	La capacidad de salida del sistema local se ve afectada y se reduce en <10%	Una falla en un elemento de los sistemas instalados que limita o reduce la capacidad de realizar el procesamiento de documentos de extremo a extremo.
Baja	Defecto menor, la capacidad de salida del sistema no se ve afectada ni se ve afectada por <10%	Defecto menor, la capacidad de salida del sistema local no se ve afectada o se ve afectada por <10%	Una falla en un elemento de los sistemas instalados que no / casi no limite o reduce la capacidad de realizar el procesamiento de documentos de extremo a extremo

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

VI.2.2 Definición de nivel de servicio en periodo de garantía para el proveedor

VI.2.2.1 Nivel de servicio para oficinas en Santo Domingo

VI.2.2.1.1 Tiempo de soporte en – sitio – Oficinas Santo Domingo

Métrica: Soporte en el sitio - Tiempo de respuesta al incidente					
Definición métrica	Medidas de tiempo para que el Consorcio EMDOC llegue al sitio o resuelva la incidencia de forma remota, después de que se active el tercer nivel de soporte por parte de la JCE.				
Horas de cobertura del servicio	Horario comercial: República Dominicana: de lunes a viernes, de 7:00 a.m. a 6:00 p.m., sábados de 8:00 am a 1:00 pm hora local (CST)				
Horas de medición		**Prioridad Crítica**	**Prioridad Alta**	**Prioridad Media**	**Prioridad Baja**
		Horas de Negocio	Horas de Negocio	Hora de Negocio	Horas de Negocios
Nivel de Servicio	El 97% In situ en Santo Domingo	2 horas	6 horas	8 horas	1 día
Metodología de Medición					
Puntos de Medición	1. El momento de la solicitud de presencia en el sitio de un ingeniero de servicio para la mesa de ayuda, es el momento en que se informa una solicitud a través de la mesa de servicio de JCE. 2. La hora de "llegada al sitio" es la hora en que el técnico de servicio documenta su llegada al sitio a través del servicio del Consorcio EMDOC.				
Estimación	"Tiempo de RESOLUCIÓN al incidente" se mide como el tiempo entre: - El momento de la notificación de la solicitud al servicio de atención a la mesa de ayuda del Consorcio EMDOC. - La hora de resolución de forma remota o en sitio.				
Frecuencia de medición	Medido para cada incidente con una presencia solicitada en el sitio.				
Fuente de Datos	Sistema de ticketing de JCE.				
Responsabilidad de medición	Sistema de ticketing de JCE el cual el Consorcio EMDOC tendrá acceso.				
Periodo de Medición	Mensual				

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

1.4. VI.2.2.2 Niveles de servicios para oficinas en República Dominicana

1.4.1. VI.2.2.2.1 Tiempo de apoyo en sitio - Oficinas De República Dominicana

Métrica: Soporte en el sitio - Tiempo de respuesta al incidente					
Definición de Métrica	Medidas de tiempo para que el Consorcio EMDOC llegue al sitio o resuelva la incidencia de forma remota, después de que se active el tercer nivel de soporte por parte de la JCE.				
Horas de cobertura del servicio	Horas de Negocios: lunes hasta viernes, 8:00 am - 5:00 pm, Tiempo Local (CST)				
Horas de medición		**Prioridad Crítica**	**Prioridad Alta**	**Prioridad Media**	**Prioridad Baja**
		Horas de Negocios	Horas de Negocios	Horas de Negocios	Horas de Negocios
Nivel de Servicio	El 97% en el sitio dentro de Santo Domingo:	4 horas	8 horas	3 días	5 días

Metodología de medición	
Puntos de medición	• El momento de la solicitud de presencia en el sitio de un ingeniero de servicio para el Consorcio EMDOC es el momento en que se informa una solicitud a través de la mesa de servicio de JCE. • La hora de "llegada al sitio" es la hora en que el técnico de servicio para el Consorcio EMDOC.
Estimación	"Tiempo de RESOLUCIÓN al Incidente" se mide como el tiempo entre: • El momento de la notificación de la solicitud al servicio de atención a la mesa de ayuda del Consorcio EMDOC. • La hora de resolución de forma remota o en sitio
Frecuencia de medición	Medido para cada Incidente con una presencia solicitada en el sitio.
Fuente de Datos	Sistema de ticketing de JCE
Responsabilidad de medición	Sistema de ticketing de JCE el cual el Consorcio EMDOC tendrá acceso.
Periodo de Medición	Mensual

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

1.4.2. VI.2.2.3 Nivel de servicio para las oficinas de los Estados Unidos de América y resto del mundo.

1.4.2.1. VI.2.2.3.1 Tiempo de apoyo en-sitio - Oficinas de los Estados Unidos de América y resto del mundo

Métrica: Soporte en el sitio - Tiempo de respuesta al incidente					
Definición de Métrica	Medidas de tiempo para que el adjudicatario llegue al sitio o resuelva la incidencia de forma remota, después de que se active el tercer nivel de soporte por parte de la JCE.				
Horas de cobertura del servicio	Consulados: de lunes a viernes, de 7:00 am a 5:00 pm, sábados de 8:00 am a 1:00 pm, según zona horaria de cada consulado.				
Horas de medición		**Prioridad Crítica**	**Prioridad Alta**	**Prioridad Media**	**Prioridad Baja**
		Horas de Negocios	Horas de Negocios	Horas de Negocios	Horas de Negocios
Nivel de Servicio	**El 97% en sitio:**	3 días	5 días	7 días	9 días
Metodología de medición					
Puntos de medición	• El momento de la solicitud de presencia en el sitio de un ingeniero de servicio para el Consorcio EMDOC es el momento en que se informa una solicitud a través de la mesa de servicio de JCE. • La hora de "llegada al sitio" es la hora en que el técnico de servicio para el Consorcio EMDOC, documenta su llegada al sitio a través del servicio del adjudicatario.				
Calculo	"Tiempo de RESOLUCIÓN al incidente" se mide como el tiempo entre: • El momento de la notificación de la solicitud al servicio de atención a la mesa de ayuda del Consorcio EMDOC. • La hora de resolución de forma remota o en sitio				
Frecuencia de medición	Medido para cada incidente con una presencia solicitada en el sitio				
Fuente de Datos	Sistema de ticketing de JCE				
Responsabilidad de medición	Sistema de ticketing de JCE el cual el Consorcio EMDOC tendrá acceso.				
Periodo de Medición	Mensual				

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

2. PLAN DE SOPORTE Y MANTENIMIENTO

2.1. Mantenimiento Preventivo de Hardware y Software

2.1.1. Actividades del Mantenimiento Preventivo

Se realizará mantenimientos preventivos a los componentes del sistema de acuerdo a los :

1. Máquinas de Impresión: mantenimiento preventivo realizado anualmente.
2. Hardware y software de los centros de datos que serán instalados por el Consorcio EMDOC, se realizarán de forma semestral. Esto incluye todo detalle para la impresión.

El Consorcio EMDOC incluye en esta propuesta, toda la infraestructura física necesaria para la implantación, ejecución y mantenimiento de la PKI, cédula de tarjeta de identificación digital, la PKI – CA, el conjunto de hardware y software en las instalaciones que se acuerden con la JCE. El contrato de mantenimiento a cotizar será de dos (2) años. A partir de los dos años, la JCE podrá renovar el mantenimiento en acuerdo con el Consorcio EMDOC.

Se ejecutarán las siguientes actividades:

1. Revisar visualmente los equipos, accesorios, conexiones y realizar un diagnóstico relacionado con el estado de su funcionamiento. Revisar alertas, logs y posibles fallas.
2. Aplicar a los componentes limpieza externa e interna, conforme los estándares de los fabricantes y las buenas prácticas.
3. Aplicar actualizaciones de firmware, drivers y software de administración o control recomendado y liberado por el fabricante de los equipos, previa autorización y aprobación del Gerente de Proyecto por la JCE.
4. Realizar el reemplazo de equipos, partes y/o piezas defectuosas o dañadas, de ser necesario, basados en los criterios de la garantía. Los equipos, partes y piezas serán nuevos de fábrica y no usadas o re- manufacturedas (Refurbished); utilizando los equipos contemplados para reemplazos requeridos inicialmente. Los reemplazos se ejecutarán en coordinación con los técnicos de la JCE y el sus oficinas en el extranjero.
5. El personal de soporte técnico del Consorcio EMDOC, realizará las pruebas de hardware y software para verificar el funcionamiento normal de los equipos, previo a la finalización del mantenimiento.

2.1.1.1. Periodicidad del mantenimiento preventivo

El mantenimiento preventivo se realizara anualmente a lo largo de los dos (2) años.

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

El primer mantenimiento se iniciará a los seis (6) meses después de aniciada la etapa 3: Operación y mantenimiento tanto para las Impresoras; Hardware y software de los centros de datos

Previa la ejecución de cada visita de mantenimiento, se presentará un cronograma que será aprobado por la JCE, con al menos 15 días de anticipación al inicio de la visita. Con este cronograma se presentará un listado de actualizaciones de hardware (drivers, firmware, otros) y software (parches de seguridad, actualizaciones, nuevas versiones, herramientas liberadas por el fabricante), que si la JCE lo considerara pertinente autorizara para que se apliquen como parte del mantenimiento preventivo.

La JCE podrá cambiar las fechas de los mantenimientos previa notificación con al menos 3 días laborables de anticipación, y aceptación del Consorcio.

2.1.1.2. Plazo de ejecución de cada visita de mantenimiento preventivo

Cada visita semestral de mantenimiento preventivo de hardware y software se realizará con la coordinación de la Gerencia de Proyecto de la JCE y la Gerencia de Proyecto del Consorcio EMDOC, en donde se realizarán los mantenimientos a todos los equipos de los centros de datos y las máquinas de impresión de las cédulas de identidad CIE y CI.

2.1.1.3. Horarios para los mantenimientos preventivos

Los horarios para ejecución de los mantenimientos preventivos en los centros de datos y las localidades de producción de cédulas se realizarán en el horario acordado con la JCE y el Consorcio EMDOC, pudiendo ser necesario laborar en períodos fuera o dentro de la jornada laboral (cuando amerite fines de semana o feriados), tanto en la República Dominicana como en el extranjero.

El horario de ejecución de los mantenimientos de las estaciones de captura de datos y entrega de cédulas y pasaportes se establecerá previa autorización y podrá ejecutarse preferentemente fuera del horario laboral o durante la jornada laboral. Esta autorización debe ser expresa por los responsables de agencia o puntos de atención sin afectar la prestación de los servicios a los ciudadanos.

Para modificar el horario de mantenimiento se debe enviar una comunicación escrita mediante carta o correo electrónico, con 24 horas de anticipación por el contacto de la JCE asignado.

2.1.1.4. Modalidad del mantenimiento preventivo

Los mantenimientos preventivos serán realizados de forma presencial y/o remota, así como también físicos o lógicos (donde aplique), tomando en cuenta las siguientes definiciones:

ITEM	LUGAR	TIPO DE MANTENIMIENTO	MODALIDAD	RESPONSABLE
Hardware y Software instalados en los Centros de Datos	República Dominicana	Físico de hardware y lógico de software	Remoto o en sitio	Consorcio EMDOC
Máquinas de Impresión (164)	República Dominicana	Físico de hardware y lógico de software	Remoto o en sitio	Consorcio EMDOC
Máquinas de Impresión (50)	Estados Unidos y Canadá	Físico de hardware y lógico de software	Remoto o en sitio	Consorcio EMDOC
Periféricos entregados por el Consorcio EMDOC a la JCE	República Dominicana	Físico de hardware y lógico de software	Remoto o en sitio	Consorcio EMDOC

La JCE, tanto en República Dominicana como en el extranjero, facilitarán al personal técnico de Consorcio EMDOC el acceso remoto a los equipos involucrados, para que se realice el respectivo mantenimiento lógico.

2.2. Informe técnico del mantenimiento preventivo

Para cada mantenimiento preventivo se realizara un Informe Técnico que contendrá la información, local o extranjera, que contendrá:

1- Punto de atención de la JCE o en el extranjero, en el cual se realizó el mantenimiento.
2- Componentes de hardware y software a los cuales se realizó el mantenimiento preventivo tanto físico como lógico.
3- Fecha y hora de Inicio del mantenimiento.
4- Fecha y hora de fin del mantenimiento.
5- Datos de contacto del responsable o técnico(s) del Consorcio EMDOC que ejecutaron el mantenimiento preventivo.
6- Datos de contacto del responsable o técnico(s) de la JCE, local o en el extranjero, que supervisaron el mantenimiento preventivo.
7- Detalle de las tareas realizadas.
8- Estado en el que quedan los componentes de hardware y software luego del mantenimiento preventivo (operando normalmente, operando con observaciones, otro).
9- El original del Acta de Entrega-Recepción de equipos, cuando corresponda por reemplazo.
10-Conclusiones
11-Recomendaciones
12-Anexos
13-Firmas de responsabilidad del informe técnico por ambas partes.

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, RD

2.3. Informe Ejecutivo periódico de mantenimiento preventivo

El Consorcio EMDOC entregará a la JCE un Informe Ejecutivo relacionado con el mantenimiento preventivo, al cierre del período de ejecución de la etapa anual. El informe contendrá la siguiente información:

1. Un cuadro consolidado de los incidentes, problemas, errores o fallos atendidos.
2. Un cuadro consolidado de equipos, partes y/o piezas reemplazadas.
3. Observaciones generales relacionadas con la ejecución del mantenimiento correctivo.
4. Conclusiones y recomendaciones generales relacionadas con la ejecución del mantenimiento correctivo.
5. Firmas de responsabilidad del informe ejecutivo.

2.4. Mano de obra, insumos, transporte, otros para la prestación del mantenimiento preventivo

La prestación del servicio de mantenimiento preventivo incluye la mano de obra, los insumos, materiales, partes, piezas o equipos, transporte y cualquier otro rubro requerido relacionado con el mismo, serán sin costo adicional para la JCE

3. MANTENIMIENTO CORRECTIVO DE HARDWARE Y SOFTWARE

3.1. Actividades del mantenimiento correctivo

El mantenimiento correctivo es un conjunto de acciones técnicas que se ejecutarán para recuperar el funcionamiento normal de uno o varios componentes de hardware y/o software entregado por el Consorcio EMDOC, cuando se presente un incidente, problema, error o fallo.

El mantenimiento correctivo puede implicar la ejecución de actividades detalladas en el mantenimiento preventivo y otras, hasta solventar la situación de excepción (incidente, problema, error o fallo que detenga por completo la operación) y dejar el componente completamente operativo en condiciones de funcionamiento normal.

3.1.1. Modalidad para el mantenimiento correctivo

El Proveedor deberá realizar el mantenimiento correctivo de forma presencial y/o remota, tomando en cuenta las siguientes consideraciones:

ITEM	LUGAR	TIPO DE MANTENIMIENTO	MODALIDAD	RESPONSABLE
Hardware y Software instalados en los Centros de Datos	República Dominicana	Físico de hardware y lógico de software	Remoto o en sitio	Consorcio EMDOC

CONSORCIO EMDOC Santo Domingo, R.D.

Máquinas de impresión (164)	República Dominicana	Físico de hardware y lógico de software	Remoto o en sitio	Consorcio EMDOC
Máquinas de impresión (53)	Estados Unidos y Canadá	Físico de hardware y lógico de software	Remoto o en sitio	Consorcio EMDOC
Periféricos entregados por el Consorcio EMDOC a la JCE	República Dominicana	Físico de hardware y lógico de software	Remoto o en sitio	Consorcio EMDOC

3.1.1.1. Horario para la prestación del servicio de mantenimiento correctivo (atención de incidentes o problemas)

El servicio de mantenimiento correctivo se ofrecerá en horario las horas de negocio de acuerdo a la prioridad del incidente, problema, error o fallo que se mencionan en esta propuesta.

3.1.1.2. Reporte o notificación de un incidente, problema, error o fallo (situación de excepción)

Las atenciones que se realizaran en las instalaciones o de manera remota, deben ser comunicadas por la mesa de soporte de la JCE, y estas deben ser reportadas al personal técnico del Consorcio EMDOC a través de la integración de la mesa de ayuda.

3.1.1.3. Mano de obra, herramientas, materiales, insumos, transporte, otros para la prestación del servicio de mantenimiento correctivo

La prestación del servicio de mantenimiento correctivo sin costo para la JCE, incluye:

1- La mano de obra especializada, las herramientas, materiales, insumos y otros requeridos.

2- El traslado de equipos, suministros, partes y/ piezas a nivel nacional o internacional, que serán entregadas en Santo Domingo a la JCE por el Consorcio EMDOC.

3.1.1.4. Equipos, partes y piezas para el mantenimiento correctivo

Con el objetivo de cumplir con los tiempos establecidos en los Niveles de Servicio:

1. Reemplazar, de forma temporal, un equipo que presente fallas por uno de su propiedad, de similares o mejores características.
2. Para el equipo de la JCE o en el extranjero que presentó fallas deberá ser arreglado y restituido por el Consorcio EMDOC

3. Los costos de transporte y de logística de este equipo corren de cuenta del Consorcio EMDOC.
4. Se incluyen los equipos, repuestos, partes y piezas que se requieran para recuperar el funcionamiento normal, que cumplan con los términos de garantías, sin costo adicional para la JCE.

3.1.1.5. Reemplazo o restitución definitiva de equipos

En aquellas situaciones que los equipos presentan daños irreparables y se requieran reemplazos de los equipos de forma definitiva estos serán nuevos, de fábrica (no re manufacturados), de la misma marca y de características técnicas iguales o superiores.

De requerir reemplazar un equipo en Ecuador de forma definitiva, será entregado en la JCE (Santo Domingo), mediante el Acta de Entrega Recepción a la JCE (Santo Domingo).

Para reemplazos de forma definitiva de una máquina de impresión en el extranjero, este equipo será entregado en la JCE (Santo Domingo) para el trámite correspondiente de alta y codificación del bien. Es responsabilidad de la JCE realizar la entrega a la localidad en el extranjero.

En el caso de acordar, una restitución de un equipo con entrega directa en un determinado en el extranjero; se entregará toda la documentación a la JCE (Santo Domingo).

3.1.1.6. Equipos de respaldo

A fin de recuperar el servicio en el menor tiempo posible, se contará con un stock de equipos para reemplazos temporales con el objetivo de cumplir con los Niveles de Servicio.

3.1.1.7. Cierre de una situación de excepción (incidente, problema, error o fallo)

Para el cierre de un ticket correspondiente a la mesa de ayuda de la JCE se adjuntarán las evidencias del caso para una situación de excepción (incidente, problema, error, fallo).

3.1.2. Informe Técnico Individual de mantenimiento correctivo por incidente, problema, error o fallo

Se elaborará un Informe Técnico de atención del cada incidente, problema, error o fallo reportado que se presente en un componente sujeto de este servicio.

El Informe Técnico contendrá los siguientes datos:
1. Localidad en el cual se realizó el mantenimiento correctivo.
2. Fecha y hora de inicio en la que se ejecutó el mantenimiento.

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

3. Fecha y hora de fin del mantenimiento.
4. Número de requerimiento generado a través de la mesa de ayuda de la JCE, o en su defecto del aperturado en la mesa de ayuda del Consorcio EMDOC.
5. Hardware y/o software sujeto del mantenimiento: marca, modelo, número de serie, código institucional, versión, fabricantes, etc.
6. Descripción de la situación de excepción atendida.
7. Procedimiento aplicado para solucionar la situación de excepción.
8. Detalle de los repuestos (materiales, partes, piezas, componentes o equipos completos) utilizados efectivamente para solucionar el incidente (en caso de aplicar).
9. Conclusiones y recomendaciones para asegurar que la situación de excepción no se vuelva a presentar.
10. Apellidos, nombres y firmas de los responsables de la atención por la JCE y/o de sus oficinas en el extranjero, que reciben el servicio y del técnico que ejecutó este servicio
11. Tiempo se atendió la notificación inicial de la situación de excepción (historia del ticket)

3.1.3. Informe Ejecutivo periódico de mantenimiento correctivo

El Consorcio EMDOC entregará a la JCE un Informe Ejecutivo relacionado con el mantenimiento correctivo, al cierre del periodo de ejecución de la etapa que cierra. El informe contendrá la siguiente información:

1. Un cuadro consolidado de los incidentes, problemas, errores o fallos atendidos.
2. Un cuadro consolidado de equipos, partes y/o piezas reemplazadas.
3. Observaciones generales relacionadas con la ejecución del mantenimiento correctivo.
4. Conclusiones y recomendaciones generales relacionadas con la ejecución del mantenimiento correctivo.
5. Firmas de responsabilidad del informe ejecutivo.

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

EMDOC
CONSORCIO

ITEM VI. A.1. INSTALACIÓN DE MÁQUINAS DE IMPRESIÓN

PARA LA CONTRATACIÓN DE LA EMPRESA QUE SE ENCARGARÁ DE SUPLIR LOS EQUIPOS, MATERIALES Y SERVICIOS PARA LA IMPRESIÓN DE LA CÉDULA DE IDENTIDAD Y ELECTORAL (CIE) Y CÉDULA DE IDENTIDAD (CI)

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.
1

EMDOC CONSORCIO

CONTENIDO

1. PLAN DE IMPLEMENTACIÓN DE IMPRESORAS 3

1.1 ESTRUCTURA DEL PLAN DE TRABAJO 3
1.1.1 *Tareas y Alcances* 3
1.1.2 *Tareas Generales para realizar por el personal del Consorcio EMDOC* 3
1.2 TAREAS IMPLEMENTACION 4
1.2.1. *Tareas de la Fase de Prechequeo.* 4
1.2.2. *Tareas para la Entrega de Impresoras.* 4
1.2.3. *Servicio de Instalación e Implementación por localidad.* 5
1.3 REQUISITOS DEL SERVICIO 5
1.3.1 *Criterios de aceptación y Cierre* 5

2. GESTIÓN DE PROYECTOS 6

2.1 INGENIEROS ESPECIALIZADOS 6
2.1.1 *Gerente de Proyecto* 6
2.1.2 *Informes de Estado* 6
2.1.3 *Reuniones de Estado* 6
2.1.4 *Calendario de Proyecto* 7
2.1.5 *Responsabilidad de ICE* 7
2.2 CONSIDERACIONES 8
2.2.1 *Proceso de revisión de documentos* 8
2.2.2 *Proceso de control de cambio* 8

3. METODOLOGÍA DE IMPLEMENTACIÓN 9

3.1 FASES DEL PROYECTO 9
3.2 FASE DE ANÁLISIS 9
3.3 FASE DE DISEÑO 9
3.4 IMPLEMENTACIÓN 9
3.5 GESTIÓN DE PROYECTO 9
3.6 COMUNICACIÓN 10
3.7 REUNIONES E INFORMES DE PROGRESO 10
3.8 PROCESO DE CONTROL DE CAMBIO 10
3.8.1 *Solicitud de Cambio* 11
3.8.2 *Proceso de una Solicitud de Cambio* 11
3.8.3 *Categorización de los Cambios* 11
3.8.4 *Proceso de Aceptación Entregables* 12
3.9 RIESGOS Y MITIGACIONES 12

CONSORCIO EMDOC

EMDOC CONSORCIO

1. Plan de Implementación de Impresoras

Este documento establece el plan de trabajo detallado para la distribución, instalación y puesta en marcha de las impresoras en cada localidad de la JCE, en República Dominicana, Estados Unidos y Canadá, Europa y los sitios de OSE de Nueva York y Madrid. El objetivo principal es garantizar una correcta implementación de las impresoras en las localidades verificando que queden operativas y funcionando correctamente en cada oficina.

1.1 Estructura del Plan de Trabajo

El Consorcio EMDOC ha dividido el plan de implementación e infraestructura en varias fases, cada una con tareas y sublareas. Los recursos, las duraciones, las dependencias y las fechas de inicio y finalización se incluyen en el Cronograma de Trabajo.

1.1.1 Tareas y Alcances

Se incluyen los servicios de instalación e implementación en todas las localidades contempladas para el proyecto (164 impresoras distribuidas en la ciudad de Santo Domingo y en el interior de la República Dominicana; 50 impresoras distribuidas en el extranjero).

1.1.2 Tareas Generales para realizar por el personal del Consorcio EMDOC

Se incluyen estas tareas por parte del Consorcio EMDOC, así como los tiempos en el cronograma:

1) **Primera fase** contiene las siguientes etapas:
    a. **Prechaqueo de instalación de cada localidad**, previo a la llegada de las impresoras e instalación del centro de datos, para verificar en cada una de las localidades cuente con todos los requisitos para la correcta instalación de las impresoras y los equipos. El objetivo es reportar oportunamente a la JCE, cualquier adecuación que sea necesaria realizar, de corregir para así mantener las áreas de forma óptima para la manipulación y operación de las impresoras y los centros de datos.
    b. **Corrección de hallazgos por JCE.** Con la finalidad de asegurar la correcta operación de las impresoras y equipos de centros de datos que entregue el Consorcio EMDOC, es necesario que la JCE realice las correcciones o mejoras previo a la segunda fase logística (distribución local e internacional).
    c. **Capacitación Operativa y Técnica** (de acuerdo como se ha indicado en el Plan de Capacitación) para el personal de la JCE se brindará por el

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

Consorcio EMDOC en la etapa 1: Implantación y puesta en marcha del proyecto.

2) **Segunda fase de logística de distribución física** de las impresoras:
   a. El reparto de **164 impresoras**. en República Dominicana, en camiones de las impresoras por todas las localidades de la JCE por el Consorcio EMDOC.
   b. Para el extranjero se incluyen las actividades de:
   - **Reexportación de 50 impresoras** al extranjero por el Consorcio EMDOC:
     - Estados Unidos (27 impresora)
     - Canadá (2 impresoras)
     - Madrid (16 impresoras) y
     - Las demás impresoras serán enviadas por la JCE desde República Dominicana.

Importante: **Distribución** a cada localidad de forma coordinada con la JCE.

Para esta distribución se requiere de la recepción de un responsable de cada localidad por la JCE o la entidad que reciba a su nombre. Con lo cual se brindará por la JCE en la fase 1, la entrega de la información de cada uno de los responsables, así como el Consorcio EMDOC brindará la información del envió de las mismas.

3) **Tercera fase de instalación e implementación de impresoras**: En paralelo con la segunda fase para cada una de las entregas, el personal técnico del Consorcio EMDOC, realizará la instalación e implementación de todas las impresoras por localidad (incluyendo reforzamiento de la capacitación brindada en la fase 1.c, ajustes y pruebas), constituyendo un requerimiento la aceptación en cada uno de las localidades la aceptación de los trabajos realizadas por el personal técnico del Consorcio EMDOC y la aceptación por parte de los responsables por la JCE en cada una de las localidades.

1.2 Tareas Implementación

1.2.1. Tareas de la Fase de Prechequeo.

1- Para cada localidad:
   a. Verificación de espacio físico, mesas, conexiones eléctricas y de datos.
   b. Documento de reporte de estado de requisitos.

1.2.2. Tareas para la Entrega de Impresoras.

1- Llevar las impresoras físicas a cada localidad y verificar que se tenga/mantenga las condiciones para instalación física para la implementación requerida.
2- Acuse de recibo por localidad por el responsable delegado por la JCE.
3- Tanto la JCE y el Consorcio EMDOC, informarán previamente los datos de los responsables por cada localidad.

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

1.2.3. Servicio de Instalación e Implementación por localidad.

En la primera semana de la fase de logística y distribución se realizará la instalación e implementación en cada sitio para las Impresoras, en función de las fechas acordadas con la a JCE, para ello el Consorcio EMDOC establecerá brigadas simultáneas, y la JCE brindará el acceso a cada uno de los sitios del personal designado por el Consorcio EMDOC, en donde se realizarán las siguientes actividades:

1- Instalación y configuración
2- Ajustes y pruebas
3- Recapacitación en sitio del personal operativo y técnico de la JCE
4- Entrega formal documentada de quien reciba por la JCE y quien entrega por el Consorcio EMDOC.

1.3 Requisitos del servicio

El Consorcio EMDOC cumplirá con los siguientes requisitos del servicio de instalación de las impresoras:

1- La capacidad del Consorcio EMDOC para brindar los servicios depende de la cooperación total y oportuna de la JCE, así como de la precisión e integridad de cualquier información y datos que JCE proporcione a Consorcio EMDOC.
2- Se incluyen en el proceso de entrega de las impresoras y varios recursos técnicos los cuales realizan la entrega de servicios en paralelo, de acuerdo con el plan.
3- La entrega programada de servicios se coordina entre el Gerente de Proyecto y la JCE.

Es importante que la JCE gestione los requisitos previos para dar el servicio en cada punto en función de las observaciones que brinda el Consorcio EMDOC por cada localidad.

El Consorcio EMDOC coordinará de forma paralela con la JCE:

1. Brindar los datos de los técnicos por el Consorcio EMDOC y quien recibirá por la JCE, de acuerdo con las fechas acordadas en conjunto.
2. Permitir el ingreso del personal del Consorcio EMDOC, en los centros de producción indicados por la JCE.

1.3.1 Criterios de aceptación y Cierre

1.3.1.1. Entregables

1- Instalación física de las Impresoras en cada localidad.
2- Configuración y ajustes de las impresoras en cada localidad.
3- Re capacitación del personal por localidad.

4- Documentación completa de los acuses de Implementaciones realizadas por localidad.

2. Gestión de Proyectos

2.1 Ingenieros Especializados

El Consorcio EMDOC asignará uno o más Soportista Técnico, quienes serán Ingenieros Especializados en cada una de las soluciones ofertadas, el cual es personal altamente calificado con las respectivas certificaciones de cada uno de los fabricantes y amplia experiencia en el despliegue de soluciones complejas.

El Consorcio EMDOC, a través de los soportistas técnicos y el personal de Gestión del Proyecto, serán los responsables del proceso de implementación, configuración y puesta a punto de cada una de las soluciones propuestas.

2.1.1 Gerente de Proyecto

El Consorcio EMDOC designará un Gerente de Proyecto ("Project Manager") para supervisar el proyecto, gestionar los recursos del proyecto y será el contacto primario del JCE con el Consorcio EMDOC con respecto a lo siguiente:

a. Gestión del alcance (solicitudes formales o informales de cambios)
b. Realización de reuniones de estado
c. Preparación de informes de estado
d. Otras actividades especificadas en esta declaración de trabajo

2.1.2 Informes de Estado

Informes de estado del proyecto serán preparados por el Gerente de Proyecto del Consorcio EMDOC para la revisión y discusión en la reunión de estado. Los informes de estado contendrán lo siguiente:

a. Resumen del estado del proyecto
b. Estado del programa contra el plan del proyecto
c. Situaciones importantes y acciones a realizar
d. Decisiones importantes tomadas en reuniones previas
e. Riesgos y acciones a realizar

2.1.3 Reuniones de Estado

Se llevará a cabo reuniones de estado del proyecto, el Gerente de Proyecto del Consorcio EMDOC y de la JCE representará a sus organizaciones en estas reuniones.

CONSORCIO EMDOC EMDOC CONSORCIO Santo Dgo. D.N.

Las reuniones de Estado incluirán:

a. Revisión del progreso contra el calendario
b. Informe para abrir ordenes de cambio
c. Revisión de temas importantes
d. Informe sobre riesgos
e. Revisar logros contra las metas esperadas

2.1.4 Calendario de Proyecto

El Consorcio EMDOC, en esta propuesta y posteriormente en las fases 1, 2 y 3 indicadas en el pliego de cargos de la JCE, a través del Gerente de Proyecto del Consorcio EMDOC, entregará un plan de proyecto que identifica y describe las actividades y tareas necesarias para proporcionar los servicios, entregables y/o configuraciones que se describe en este documento. Así como los cambios significativos (es decir, cambios en la fecha final o una adición de horas para el calendario del proyecto).

La JCE será responsable de revisar y aprobar el contenido de la versión inicial de la programación del proyecto según el proceso de revisión del documento definido en este documento. Una vez aceptado, el calendario del proyecto se convertirá en la línea de base contra el cual se medirán los entregables y las prestaciones de los servicios. Cambios en el calendario del proyecto se revisarán en el proceso de cambio.

2.1.5 Responsabilidad de JCE

2.1.5.1. Asignar a un promotor del proyecto

1- Con disponibilidad durante toda la vida del proyecto.
2- Actuar como punto de escalación cuando los conflictos no pueden ser resueltos por el director del proyecto.

2.1.5.2. Asignar a un Gerente de Proyecto

1- Responsable de comunicar todos los aspectos de este proyecto al JCE.
2- Autorizado para la toma de las decisiones en relación con el proyecto, incluyendo la identificación y asignación de recursos del JCE.
3- Disponible para el personal de consultoría del Consorcio EMDOC y la JCE durante toda la vida del proyecto.
4- Autorizados para firmar informes de estado, aprobar horas del Consultor y aprobar los cambios de proyecto.
5- Coordinar todos los calendarios de reuniones o entrevistas.
6- Responsable de la aceptación de entregables y verificar el cumplimiento de cada entregable con los criterios de aceptación como definido.
7- Autorizado para aprobar los cambios de proyecto.

Asignar a los gerentes y demás personal, según sea el caso, trabajar con el Consorcio EMDOC y la JCE durante toda la vida del contrato.

Se espera la participación de la JCE a lo largo de las fases del ciclo de vida del proyecto, por ejemplo, la interacción oportuna para las actividades de análisis y diseño, implementación y pruebas.

La JCE deberá revisar los informes de estado o de la aceptación, conforme a lo dispuesto y proporcionar aceptación u observaciones según lo especificado.

La JCE brindará el Acceso al personal del Consorcio EMDOC, a las instalaciones (localidades o edificio) de la JCE, facilidades de equipo, sistemas, contraseñas, etc., según sea necesario, durante el horario normal, así como después de horas, si es necesario para completar las actividades por el personal del Consorcio EMDOC.

La JCE proporcionará un área de trabajo adecuado acorde con el número de consultores en el sitio. El área de trabajo incluye escritorios, sillas, teléfonos y acceso a la red internet para el personal del Consorcio EMDOC a través de una VPN.

2.2 Consideraciones

2.2.1 Proceso de revisión de documentos

El Gerente de Proyecto del Consorcio EMDOC y sus Consultores pueden programar sesiones de trabajo, que incluirá al personal de la JCE y el Consorcio EMDOC, para afinar el documento de proyecto, como está escrito.

El Gerente de Proyecto es responsable de consolidar comentarios de la JCE y proporcionar una versión claramente marcada del proyecto de documento al Consultor y al Gerente de Proyecto de Consorcio EMDOC. La entrega de la versión final de un documento constituirá la aceptación del JCE de este.

2.2.2 Proceso de control de cambio

El proceso de control de cambio en general se llevará a cabo como se ilustra en la siguiente figura. La JCE o el Consorcio EMDOC puede iniciar un cambio, por escrito, para el proyecto. Se evaluará el cambio, y se identificará el impacto de cualquier actividad del proyecto.

Todos los cambios deben ser mutuamente acordados por las partes. Una vez aprobado, se implementarán los cambios en el proyecto inicial y se acordedarán los plazos en los cuales la JCE, podrá notificar estos cambios.

3. Metodología de Implementación

3.1 Fases del proyecto

El ciclo de los servicios profesionales provistos por el Consorcio EMDOC se basa en la secuenciación de la fase de Análisis, fase de Diseño y fase de Implementación, las mismas son ejecutadas tomando en consideración el empleo de las mejores prácticas y la experiencia obtenida a través de las distintas soluciones entregadas y su puesta en productivo de manera satisfactoria.

3.2 Fase de Análisis

Para la fase de análisis representantes de la JCE y los especialistas del Consorcio EMDOC, se ponen de acuerdo para coordinar y llevar a cabo las distintas sesiones técnicas, necesarias para comprender más fondo el escenario actual partiendo de las informaciones provistas por la JCE y los levantamientos de la infraestructura existente.

3.3 Fase de Diseño

El Diseño incorporará los requerimientos de las soluciones adquiridas por la JCE indicadas en la propuesta. El diseño resultante se corresponde a las informaciones y levantamientos realizados durante la fase de Análisis.

3.4 Implementación

En esta fase se ejecuta el alcance de las actividades señaladas en la propuesta del Consorcio EMDOC. De esta fase se deriva el documento de implementación as built, el cual, junto a los servicios profesionales de implementación, conforman los entregables que contienen el detalle del producto final a recibir por la JCE.

3.5 Gestión de Proyecto

El Consorcio EMDOC asignará un Gerente de Proyecto y pondrá a disposición de la JCE su oficina para la gestión del proyecto, PMO. El Gerente del Proyecto llevará a cabo reuniones periódicas para revisar el estado del proyecto, medir el progreso de las tareas críticas específicas y definir las alternativas ante los posibles imprevistos que surjan durante el desarrollo del proyecto. Dichas reuniones periódicas se celebrarán partiendo de la frecuencia acordada con la JCE.

Se sugiere a la JCE designar igualmente, un Gerente de Proyecto, el cual, junto al Gerente de Proyecto asignado por el Consorcio EMDOC, serán los principales representantes para la administración y otros asuntos relativos a las actividades del proyecto.

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

3.6 Comunicación

Las siguientes tareas serán realizadas por el Gerente de Proyecto del Consorcio EMDOC:

1- Mantener la comunicación con el Gerente de Proyecto de la JCE.
2- Preparar y presentar al Gerente de Proyecto de la JCE los informes periódicos de situación.
3- Coordinar y manejar las tareas/actividades relacionadas al alcance de proyecto asignando las fechas respectivas para su ejecución.
4- Definir entre las partes los documentos de entregables que se requieren.
5- Preparar y compartir las minutas de las reuniones celebradas.

3.7 Reuniones e Informes de Progreso

El Consorcio EMDOC entregará informes de progreso según la frecuencia acordada con la JCE. Los informes serán compartidos al Gerente de Proyecto de la JCE, vía correo electrónico o entregas físicas en ventanilla de recepción de documentos. El informe estará compuesto de los campos listados a continuación:

1- Datos generales del proyecto.
2- Progreso general obtenido.
3- Logros obtenidos durante el periodo transcurrido.
4- Tareas/actividades planificadas para el próximo periodo.
5- Áreas de Atención.
6- Riesgos identificados.

La JCE participará y apoyará las reuniones de revisión de proyecto con el Consorcio EMDOC y sus respectivos Gerentes de Proyectos y equipos de trabajo. Las revisiones cubrirán los aspectos técnicos, itinerarios de trabajos, y asignación de recursos para el proyecto. Se hará énfasis en los logros obtenidos y tareas finalizadas del periodo que se reporta, actividades previstas para el periodo en curso, y la identificación y resolución de todas las áreas de atención. La revisión se llevará a cabo en la fecha y lugar a determinarse conjuntamente por los Gerentes de Proyectos del Consorcio EMDOC y la JCE. La agenda y las minutas de cada reunión, se elaborarán manteniendo el acuerdo en común por los Gerentes de Proyectos del Consorcio EMDOC y la JCE.

3.8 Proceso de Control de Cambio

El objetivo central de este proceso es garantizar que los cambios que se adopten sean aquellos que realmente requiere el proyecto y que estén alineados con el logro de los objetivos definidos para el pliego de cargos y sus aclaraciones de la JCE y propuesta presentada por el Consorcio EMDOC, descartando todos aquellos cambios que no sean relevantes o que no signifiquen una mejora importante durante el contrato. Dentro del procedimiento el rol central es el del Gerente de Proyecto de cada una de LAS PARTES. La persona que desempeñe este rol será designada conjuntamente por los Representantes de la JCE y el Consorcio EMDOC.

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

3.8.1 Solicitud de Cambio

En principio, los interesados o responsables autorizados a solicitar un cambio en cualquier momento durante la ejecución del proyecto. La solicitud de cambio debe realizarse por escrito empleando el formulario de solicitud de cambio. Dicho formulario está compuesto por los campos siguientes:

1- Solicitante del cambio.
2- Descripción del cambio.
3- Justificación del cambio.
4- Identificación preliminar de componentes afectados.
5- Impacto del cambio.

3.8.2 Proceso de una Solicitud de Cambio

El Gerente de Proyecto se encargará que cada solicitud se evalueda hasta que esta, sea aprobada o rechazada en el marco de esta propuesta y el contrato. El curso normal de esa solicitud se describe a continuación:

1- El Gerente de Proyectos identificará quién o quiénes están mejor calificados para evaluar cada cambio solicitado y solicitar de ellos una evaluación.
2- La evaluación funcional debe categorizar el cambio y calcular su impacto desde el punto de vista del negocio.
3- Prioridad que tiene el cambio para la JCE (Alta o baja).
4- Prioridad que tiene el cambio para la función (Alta o baja).
5- Tipo de impacto que ese cambio tendrá sobre el proyecto.
6- Tipo de impacto que ese cambio tendrá sobre otras áreas del negocio.
7- Qué trabajo o esfuerzo adicional facturable debe hacerse si se efectuara el cambio.

El Gerente de Proyecto enviaré a los Representantes de la JCE, la solicitud de cambio y los resultados de las evaluaciones, con el fin de que sea procesada de acuerdo con su magnitud e impacto.

El Gerente de Proyecto de la JCE y el Gerente de Proyecto EMDOC convocarán y dirigirán las reuniones que sean necesarias para aprobar o rechazar la solicitud de cambios.

También, dada su responsabilidad, ambos Gerentes del Proyecto llevarán a cabo todas las acciones acordadas que sean necesarias para hacer efectivos los cambios que hayan sido aprobados.

3.8.3 Categorización de los Cambios

El Gerente de Proyecto de la JCE y el Gerente de Proyecto del Consorcio EMDOC efectuarán un análisis preliminar para calificar el cambio.

Calificaciones posibles:

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

1- Cambio Menor: Se considerará un "Cambio Menor" a aquel requerimiento que esté enmarcado en el alcance del Servicio y se encuentre debidamente definido en los pliegos de cargos y Consultas y Respuestas publicados por la JCE, propuesta entregada por el Consorcio EMDOC y el contrato sigando entre LAS PARTES.
2- Cambio Mayor: Se considerará un "Cambio Mayor" a aquel requerimiento que no esté enmarcado en el alcance del Servicio y afecte los costos y/o los cronogramas del proyecto. Cambio Sustancial: Se considerará un "Cambio Sustancial" a aquel requerimiento que no esté enmarcado en el alcance del Servicio y/o afecte sustancialmente los cronogramas del proyecto y a los pliegos de cargos y Consultas y Respuestas publicados por la JCE, propuesta entregada por el Consorcio EMDOC y el contrato sigando entre LAS PARTES.

3.8.4 Proceso de Aceptación Entregables

Una forma de aceptación de entregables será provista por el Gerente de Proyecto del Consorcio EMDOC para el reconocimiento de aceptación de cada servicio e hitos completados. La JCE dará acuse de recibo de la aceptación del entregable firmando la forma de aceptación de entregables.

3.9 Riesgos y mitigaciones

Riesgos	Mitigaciones
Disponibilidad en las sesiones de trabajo	Acordar tiempos convenientes para los involucrados en el equipo de trabajo.
Proporcionar acceso y la información requerida de manera oportuna	Identificar al inicio del proyecto los roles clave dentro de la implementación para mantener un contacto directo con los responsables de los accesos y administración de algunos servicios dentro de la infraestructura tecnológica.

215

EMDOC
CONSORCIO

ITEM VI. PARTE A - PROPUESTA INFRAESTRUCTURA CENTRO DE DATOS

PARA LA CONTRATACIÓN DE LA EMPRESA QUE SE ENCARGARÁ DE SUPLIR LOS EQUIPOS, MATERIALES Y SERVICIOS PARA LA IMPRESIÓN DE LA CÉDULA DE IDENTIDAD Y ELECTORAL (CIE) Y CÉDULA DE IDENTIDAD (CI)

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo R.D.

EMDOC

CONTENIDO

1. EQUIPOS ACTIVOS DE LA SOLUCIÓN PROPUESTA 3

1.1 DESCRIPCIÓN DE LA SOLUCIÓN PROPUESTA 3

1.1.1 Centro de Datos Principal 3

1.1.2 CENTRO DE DATOS ALTERNO 6

1.1.3 Licenciamiento Incluido 10

1.1.4 Mantenimiento y Soporte 10

1.2 DIAGRAMA DE LA SOLUCIÓN 11

1.2.1 Descripción 12

2. PLAN DE TRABAJO IMPLEMENTACIÓN INFRAESTRUCTURA EN CENTROS DE DATOS 14

2.1 ESTRUCTURA DEL PLAN DE TRABAJO 14

2.2 TAREAS Y ALCANCES 14

2.2.1 Tareas Generales 14

2.2.2 Tareas de Implementación e Instalación 15

3. JUSTIFICACIÓN 16

4. JUSTIFICACIÓN DEL PLAN DE RECUPERACIÓN Y RESPALDO 19

5. CAPACITACIÓN 21

5.1 VEEAM BACKUP AND REPLICATION 12.1 21

5.1.1 Objetivos de la Capacitación 22

5.1.2 Temario de la Capacitación 22

5.2 VMWARE VSPHERE: OPERATE, SCALE AND SECURE 23

5.2.1 Objetivos de la Capacitación 23

5.2.2 Temario de la Capacitación 24

5.3 HPE PROLIANT GEN11 SERVER MANAGEMENT WITH ILO 6 24

5.3.1 Objetivos de la Capacitación 25

5.3.2 Temario de la Capacitación 25

6. PREMISAS Y ENTREGABLES 26

CONSORCIO EMDOC
EMDOC CONSORCIO
Santo Domingo, R.D.

1. Equipos Activos de la Solución Propuesta

Nuestra propuesta incluye toda la infraestructura de hardware para soportar la solución de software para la impresión de la nueva cedula de identidad y electoral (CIE) y cedula de identidad (CI).

1.1 Descripción de la solución propuesta

La arquitectura está conformada por dos sitios que actuaran en configuración altamente disponible y redundante de cada uno; esto para garantizar la operación continua ante desastres o contingencias que se pudieran presentar. Nuestra propuesta incluye el equipamiento necesario para la operación de la solución propuesta, tanto para el sitio principal como para el alterno. A continuación, se detallan los componentes incluidos en nuestra oferta.

1.1.1 Centro de Datos Principal

Rack HPe 42U

Cantidad: uno (1)

Será utilizado para instalar los equipos activos de la solución propuesta. Incluye accesorios de fijación de este, así como PDUs de interconexión eléctrica de los equipos activos hasta la toma eléctrica suministrada por la JCE dentro del rack.

HPE Aruba Networking CX 6300M 24-port SFP+

Cantidad: dos (2)

Será utilizado para la interconexión de los elementos activos de la solución propuesta e integración a la red existente del cliente. Se requiere interconexión de los uplinks (mínimo cuatro por equipo) a cualquiera de las opciones soportadas (10/25/40/50/100 GbE) para la integración aguas arriba de la plataforma.

Fortinet FAD420F Balanceadores

Cantidad: dos (2)

Serán utilizados para balancear la carga para los servicios entrantes en los diferentes nodos de servicio de la infraestructura propuesta.

Hardware para la Plataforma PKI para grabado chip de cédulas - Servidores HPe Proliant DL380 Gen11

Cantidad: dos (2)

Equipamiento activo que hospedará la solución de PKI para grabado de chip de las cedulas, así como la infraestructura de administración de virtualización de la solución.
Cada servidor incluye:

- 2 x Procesadores Intel Xeon-G 6426Y 16 Cores a 2.5GHz
- 256GB de RAM
- 2 x HPE 240GB SATA RI SFF BC MV SSD

- 3 x HPE 3.84TB SATA RI SFF BC MV SSD
- 1 x Tarjeta Broadcom 57412 10GbE 2p
- Incluye todos los SFP requeridos y cables LC/LC de 5 metros
- Fuentes Redundantes

Hardware para la Plataforma Mobile - Servidores HPe Proliant DL360 Gen11

Cantidad: dos (2)

Equipamiento activo que hospedará la solución de Mobile ID.

Cada servidor incluye:

- 2 x Procesadores Intel Xeon-G 6426Y 16 Cores a 2.5GHz
- 384GB de RAM
- 2 x HPE 240GB SATA RI SFF BC MV SSD
- 3 x HPE 3.84TB SATA RI SFF BC MV SSD
- 1 x Tarjeta Broadcom 57412 10GbE 2p
- 1 x tarjeta quad port 1Gbps
- Incluye todos los SFP requeridos y cables LC/LC de 5 metros
- Fuentes Redundantes

Hardware para la Plataforma PKI Ciudadana - Servidoras HPe Proliant modelos DL360 Gen11 (AC Raiz)

Cantidad: uno (1)

Equipamiento activo que hospedará la entidad AC Raíz de la PKI Ciudadana.

Este servidor incluye:

- 1 x Procesadores Intel Xeon-S 4410Y 12 Cores a 2.0GHz
- 32GB de RAM
- 2 x HPE 960GB NVMe SSD
- Incluye todos los SFP requeridos y cables LC/LC de 5 metros
- Fuentes Redundantes

Hardware para la Plataforma PKI Ciudadana - Servidores HPe Proliant modelos DL360 Gen11 (AC Subordinadas)

Cantidad: dos (2)

Equipamiento activo que hospedará la entidad AC Subordinadas de la PKI Ciudadana.

Cada servidor incluye:

- 1 x Procesadores Intel Xeon-S 4416+ 20 Cores a 2.0GHz
- 64GB de RAM
- 2 x HPE 960GB NVMe SSD
- Incluye todos los SFP requeridos y cables LC/LC de 5 metros
- Fuentes Redundantes

Hardware para la Plataforma PKI Ciudadana - Servidores HPe Proliant modelos DL360 Gen11 (Vertical de Firma)

Cantidad: dos (2)

Equipamiento activo que hospedará la entidad Vertical de Firmas de la PKI Ciudadana.

Cada servidor incluye:

- 2 x Procesadores Intel Xeon-G 6548N+ 32 Cores a 2.8GHz

219

- 128GB de RAM
- 2 x HPE 1.92TB NVMe SSD
- Incluye todos los SFP requeridos y cables LC/LC de 5 metros
- Fuentes Redundantes

Hardware para la Plataforma PKI Ciudadana - Servidores HPe Proliant modelos DL360 Gen11 (SeguriSign, SeguriNotary, OCSP)

Cantidad: dos (2)

Equipamiento activo que hospedará la entidad SeguriSign, SeguriNotary y OCSP de la PKI Ciudadana.

Cada servidor incluye:

- 2 x Procesadores Intel Xeon-G 6548N+ 32 Cores a 2.8GHz
- 128GB de RAM
- 2 x HPE 1.92TB NVMe SSD
- Incluye todos los SFP requeridos y cables LC/LC de 5 metros
- Fuentes Redundantes

Hardware para Aplicaciones (POC)- Servidores HPe Proliant DL20 Gen11

Cantidad: uno (1)

Equipamiento activo que hospedará la de POC de los componentes DB, APP, Auth de los servicios.

Este servidor incluye:

- 1 x Procesadores Intel Xeon E-2468 8 Cores a 2.0GHz
- 64GB de RAM
- 2 x HPE 1TB HDD
- Incluye todos los SFP requeridos y cables LC/LC de 5 metros

Hardware para Aplicaciones (Ambiente Redundante)- Servidores HPe Proliant DL380 Gen11

Cantidad: dos (2)

Equipamiento activo que hospedará la solución de Mobile ID.

Cada servidor incluye:

- 2 x Procesadores Intel Xeon-G 5418Y 24 Cores a 2.0GHz
- 256GB de RAM
- 4 x HPE 480GB SATA RI SFF BC MV SSD
- 4 x HPE 1.6TB SATA RI SFF BC MV SSD
- Incluye todos los SFP requeridos y cables LC/LC de 5 metros
- Fuentes Redundantes



Appliance de Backup HPe StoreOnce 3660

Cantidad: uno (1)

Solución de respaldo para realizar las copias de seguridad necesarios para garantizar la operación ante desastres de la arquitectura propuesta.

Incluye capacidad de backup para 96TB

Unidad de Almacenamiento HPE MSA 2062 10GbE iSCSI

Cantidad uno (1)
Será utilizado como unidad de almacenamiento de toda la infraestructura para proveer servicios de datos estructurados y no estructurados a la plataforma.
Incluye:

- 16 x HPE MSA 3.84TB SAS RI SFF M2 SSD
- 4 x Puertos 10Gbs

Hardware para Backup y Proxy VEEAM - Servidores HPe Proliant modelos DL360 Gen11

Cantidad: dos (2)
Equipamiento activo para la administración de la solución de backup y realización de estos a través de agentes y/o funciones nativas de la plataforma de virtualización.
Cada servidor incluye:

- 1x Procesador Intel Intel Xeon Gold 5416S 2.0GHz
- 32GB de RAM
- 2x HPE 960GB SATA RI SFF BC MV SSD
- 1 x tarjeta doble port 1Gbps
- 1 x tarjeta doble port 10Gbps
- Incluye todos los SFP requeridos y cables LC/LC de 5 metros
- Fuentes Redundantes

Módulos criptográficos

- 1 Utimaco CryptoServer CP5 Se52PCIe, CC certified acc. EN419221-5
- 1 Utimaco CC eIDAS on CryptoServer General Purpose Network HSM SecurityServer Se100 LAN V5
- Se incluyen también 10 Fichas criptográficas USB (material de claves y certificados de autenticación de clientes), para el equipo de administrac
- 2 módulos de seguridad criptográfica CryptoServer CP5 Se 500 de Utimaco, con cumplimiento Common Criteria, eIDAS y FIPS 140-2 Nivel 3 o superior, que cumplen con las características descritas en el apartado Hardware Criptográfico, considerar impuestos, 2 equipos serán para ambiente productivo y 1 equipo para ambiente DRP.
- 1 módulos de seguridad criptográfica CryptoServer CP5 Se 12, con cumplimiento Common Criteria, eIDAS y FIPS 140-2 Nivel 3 o superior, que cumplen con las características descritas en el apartado Hardware Criptográfico, considerar impuestos, 1 equipo será para ambiente productivo y 1 equipo para ambiente DRP.

1.1.2 CENTRO DE DATOS ALTERNO

Rack HPe 42U

Cantidad: uno (1)
Será utilizado para instalar los equipos activos de la solución propuesta. Incluye accesorios de fijación de este, así como PDUs de interconexión eléctrica de los equipos activos hasta la toma eléctrica suministrada por la JCE dentro del rack.

EMDOC

HPE Aruba Networking CX 6300M 24-port SFP+

Cantidad. dos (2)

Será utilizado para la interconexión de los elementos activos de la solución propuesta e integración a la red existente del cliente. Se requiere interconexión de los uplinks (mínimo cuatro por equipo) a cualquiera de las opciones soportadas (10/25/40/50/100 GbE) para la integración aguas arriba de la plataforma.

Fortinet FAD420F Balanceadores

Cantidad. dos (2)

Serán utilizados para balancear la carga para los servicios entrantes en los diferentes nodos de servicio de la infraestructura propuesta.

Hardware para la Plataforma PKI para grabado chip de cédulas - Servidores HPe Proliant DL380 Gen11

Cantidad: dos (2)

Equipamiento activo que hospedará la solución de PKI para grabado de chip de las cedulas, así como la infraestructura de administración de virtualización de la solución.
Cada servidor incluye:

- 2 x Procesadores Intel Xeon-G 6426Y 16 Cores a 2.5GHz
- 256GB de RAM
- 2 x HPE 240GB SATA RI SFF BC MV SSD
- 3 x HPE 3.84TB SATA RI SFF BC MV SSD
- 1 x Tarjeta Broadcom 57412 10GbE 2p
- Incluye todos los SFP requeridos y cables LC/LC de 5 metros
- Fuentes Redundantes

Hardware para la Plataforma Mobile - Servidores HPe Proliant DL360 Gen11

Cantidad: uno (1)

Equipamiento activo que hospedará la solución de Mobile ID.
Este servidor incluye:

- 2 x Procesadores Intel Xeon-G 6426Y 16 Cores a 2.5GHz
- 384GB de RAM
- 2 x HPE 240GB SATA RI SFF BC MV SSD
- 3 x HPE 3.84TB SATA RI SFF BC MV SSD
- 1 x Tarjeta Broadcom 57412 10GbE 2p
- 1 x tarjeta quad port 1Gbps
- Incluye todos los SFP requeridos y cables LC/LC de 5 metros
- Fuentes Redundantes

CONSORCIO EMDOC EMDOC Santo Domingo R.D.

Hardware para la Plataforma PKI Ciudadana - Servidores HPe Proliant modelos DL360 Gen11 (AC Raiz)

Cantidad: uno (1)

Equipamiento activo que hospedará la entidad AC Raíz de la PKI Ciudadana
Este servidor incluye:

- 1 x Procesadores Intel Xeon-S 4410Y 12 Cores a 2.0GHz

- 32GB de RAM
- 2 x HPE 960GB NVMe SSD
- Incluye todos los SFP requeridos y cables LC/LC de 5 metros
- Fuentes Redundantes

Hardware para la Plataforma PKI Ciudadana - Servidores HPe Proliant modelos DL360 Gen11 (AC Subordinadas)

Cantidad: uno (1)

Equipamiento activo que hospedará la entidad AC Subordinadas de la PKI Ciudadana.

Este servidor incluye:

- 1 x Procesadores Intel Xeon-S 4416+ 20 Cores a 2.0GHz
- 64GB de RAM
- 2 x HPE 960GB NVMe SSD
- Incluye todos los SFP requeridos y cables LC/LC de 5 metros
- Fuentes Redundantes

Hardware para la Plataforma PKI Ciudadana - Servidores HPe Proliant modelos DL360 Gen11 (Vertical de Firma)

Cantidad: uno (1)

Equipamiento activo que hospedará la entidad Vertical de Firmas de la PKI Ciudadana.

Este servidor incluye:

- 2 x Procesadores Intel Xeon-G 6548N+ 32 Cores a 2.8GHz
- 128GB de RAM
- 2 x HPE 1.92TB NVMe SSD
- Incluye todos los SFP requeridos y cables LC/LC de 5 metros
- Fuentes Redundantes

Hardware para la Plataforma PKI Ciudadana - Servidores HPe Proliant modelos DL360 Gen11 (SeguriSign, SeguriNotary, OCSP)

Cantidad: uno (1)

Equipamiento activo que hospedará la entidad SeguriSign, SeguriNotary y OCSP de la PKI Ciudadana.

Este servidor incluye:

- 2 x Procesadores Intel Xeon-G 6548N+ 32 Cores a 2.8GHz
- 128GB de RAM
- 2 x HPE 1.92TB NVMe SSD
- Incluye todos los SFP requeridos y cables LC/LC de 5 metros
- Fuentes Redundantes

Hardware para Aplicaciones (POC)- Servidores HPe Proliant DL20 Gen11

Cantidad: uno (1)

Equipamiento activo que hospedará la de POC de los componentes DB, APP, Auth de los servicios.

Este servidor incluye:

- 1 x Procesadores Intel Xeon E-2468 8 Cores a 2.6GHz
- 64GB de RAM

- 2 x HPE 1TB HDD
- Incluye todos los SFP requeridos y cables LC/LC de 5 metros

Hardware para Aplicaciones (Ambiente Redundante)- Servidores HPe Proliant DL360 Gen11

Cantidad: uno (1)

Equipamiento activo que hospedará la solución de Mobile ID.
Este servidor incluye:

- 2 x Procesadores Intel Xeon-G 5418Y 24 Cores a 2.0GHz
- 256GB de RAM
- 4 x HPE 480GB SATA RI SFF BC MV SSD
- 4 x HPE 1.6TB SATA RI SFF BC MV SSD
- Incluye todos los SFP requeridos y cables LC/LC de 5 metros
- Fuentes Redundantes

Appliance de Backup HPe StoreOnce 3660

Cantidad: uno (1)

Solución de respaldo para realizar las copias de seguridad necesarios para garantizar la operación ante desastres de la arquitectura propuesta.
Incluye capacidad de backup para 96TB

Unidad de Almacenamiento HPE MSA 2062 10GbE iSCSI

Cantidad: uno (1)

Será utilizado como unidad de almacenamiento de toda la infraestructura para proveer servicios de datos estructurados y no estructurados a la plataforma.
Incluye:

- 16 x HPE MSA 3.84TB SAS RI SFF M2 SSD
- 4 x Puertos 10Gbs

Hardware para Backup y Proxy VEEAM - Servidores HPe Proliant modelos DL360 Gen11

Cantidad: dos (2)

Equipamiento activo para la administración de la solución de backup y realización de estos a través de agentes y/o funciones nativas de la plataforma de virtualización.
Cada servidor incluye:

- 1x Procesador Intel Intel Xeon Gold 5416S 2.0GHz
- 32GB de RAM
- 2x HPE 960GB SATA RI SFF BC MV SSD
- 1 x tarjeta doble port 1Gbps
- 1 x tarjeta doble port 10Gbps
- Incluye todos los SFP requeridos y cables LC/LC de 5 metros
- Fuentes Redundantes

Módulos criptográficos

- 1 Utimaco CryptoServer CP5 Se52PCIe, CC certified acc. EN419221-5

- 1 Ultmaco CC eIDAS on CryptoServer General Purpose Network HSM SecurityServer Se100 LAN V5
- Se incluyen también 10 Fichas criptográficas USB (material de claves y certificados de autenticación de clientes), para el equipo de administrac
- 1 módulos de seguridad criptográfica CryptoServer CP5 Se 500 de Ultmaco, con cumplimiento Common Criteria, eIDAS y FIPS 140-2 Nivel 3 o superior, que cumplen con las características descritas en el apartado Hardware Criptográfico, considerar impuestos, 2 equipos serán para ambiente productivo y 1 equipo para ambiente DRP.
- 1 módulos de seguridad criptográfica CryptoServer CP5 Se 12, con cumplimiento Common Criteria, eIDAS y FIPS 140-2 Nivel 3 o superior, que cumplen con las caracteristicas descritas en el apartado Hardware Criptográfico, considerar impuestos, 1 equipo será para ambiente productivo y 1 equipo para ambiente DRP.

En este caso, la JCE es responsable de suministrar el espacio requerido para la instalación del rack que hospedará todos los equipos activos de la solución tanto en el centro de datos primario, como en el secundario. En adición, es responsable de garantizar la conectividad eléctrica y de datos requerida para la correcta operación de la solución

1.1.3 Licenciamiento Incluido

Se incluye el siguiente licenciamiento para todos los equipos

- Red Hat Enterprise Linux Server, Premium (Physical or Virtual Nodes)
- vMware Standard
- Veeam Data Platform Premium. 3 Years Subscription Upfront Billing & Production (24/7) Support. Public Sector
- PostgreSQL Database

Nota: Todos los softwares incluidos son de tipo suscripción por treinta y seis (36) meses.

1.1.4 Mantenimiento y Soporte

Nuestra propuesta incluye soporte y garantías directo del fabricante según lo siguiente:

Garantía

- El hardware incluye garantía de hardware del fabricante por sesenta (60) meses con reemplazo de partes y almacén de piezas local.
- El Consorcio EMDOC brindará el servicio de reemplazo de partes una vez estas sean entregadas por el fabricante en las instalaciones de la JCE.

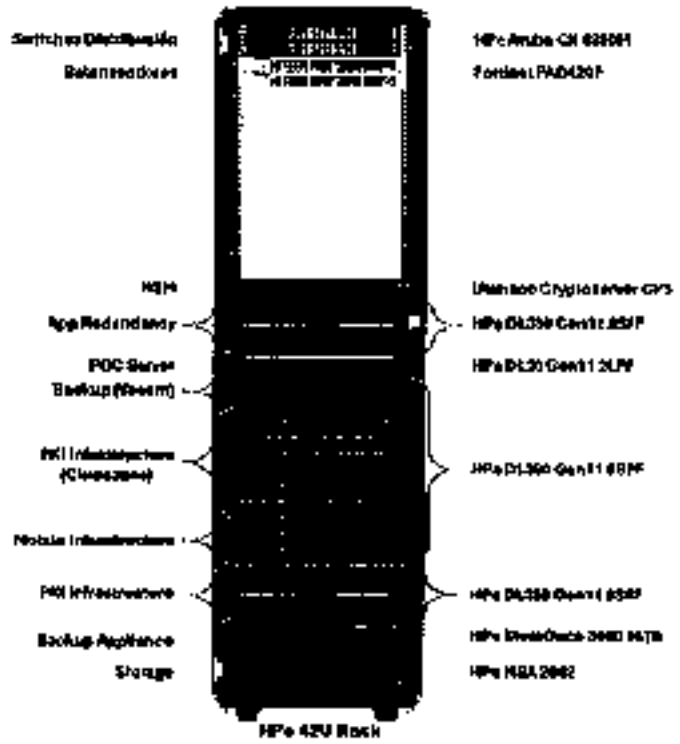
Soporte

- Se incluye soporte para el hardware, sistemas operativos y base de datos por (60) meses con SLA 7x24x365.
- El soporte incluye atención nivel 1 y 2 por parte del Consorcio EMDOC. El soporte nivel 3 será brindado por el fabricante.

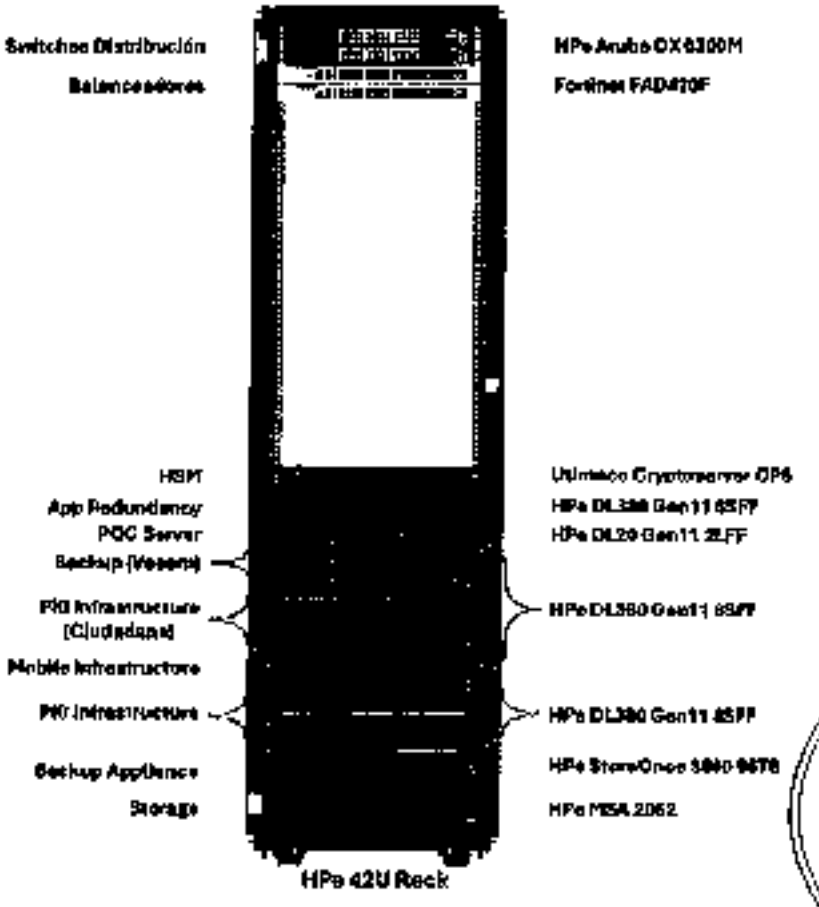
- El Consorcio EMDOC estará realizando visitas bianuales para el correcto mantenimiento preventivo de la Infraestructura propuesta. Este mantenimiento preventivo incluye:
  - Monitoreo de temperatura y consumo eléctrico.
  - Detección de fallos en componentes internos (discos, memorias, tarjetas).
  - Revisión de logs de eventos críticos.
  - Verificación de alertas en los sistemas de gestión/administración
  - Revisión de firmware (BIOS, controladoras, tarjetas de red).
  - Evaluación de consumo de recursos (CPU, RAM, discos).
  - Verificación de snapshots y replicación de datos.
  - Evaluación de la capacidad utilizada y planificación de expansión.
  - Aplicación de parches de seguridad y actualizaciones menores.
  - Verificación de servicios críticos en ejecución.

1.2 Diagrama de la Solución

La solución está compuesta por dos gabinetes instalado en cada uno de los centros de datos, primario y secundario de la JCE.
En el caso del Centro de Datos Primario se tiene:



Para el Centro de Datos Primario se estará consumiendo un total de 30 unidades de rack, quedando libres unas 12 unidades de rack que podrán ser utilizadas para futuro crecimiento y expansión de la plataforma.
En el caso del Centro de Datos Secundario se tiene:



Para el Centro de Datos Primario se estará consumiendo un total de 24 unidades de rack, quedando libres unas 18 unidades de rack que podrán ser utilizadas para futuro crecimiento y expansión de la plataforma.

1.2.1 Descripción

Se contará con un rack HPe de 42U en cada localidad. El Rack HPe 42U permitirá contar con una infraestructura tecnológica de alta disponibilidad diseñada para optimizar la gestión de redes, aplicaciones, seguridad y almacenamiento de datos en entornos empresariales y gubernamentales. Está compuesto por equipos de última generación que garantizan rendimiento, seguridad y escalabilidad.

HPe Aruba CX 6300M (Switch de Distribución)
Switch de red de alto rendimiento diseñado para la distribución eficiente del tráfico.
Beneficios. Proporciona conectividad rápida y confiable con capacidades avanzadas de automatización y administración.
Seguridad: Soporte para políticas de acceso, segmentación de tráfico y protección contra ataques de red.
Redundancia: Capacidad de stacking y enlaces redundantes para evitar fallos en la red.

Fortinet FAD420F (Balanceador de Carga)
Dispositivo de balanceo de carga para distribuir tráfico entre servidores y mejorar la disponibilidad de servicios.
Beneficios: Optimiza el rendimiento, mejora la experiencia del usuario y reduce el tiempo de inactividad.
Seguridad: Protección contra ataques DDoS y control de tráfico cifrado.
Redundancia: Distribución inteligente del tráfico para evitar sobrecargas en servidores críticos.

Utimaco Cryptoserver CP5 (HSM – Hardware Security Module)
Módulo de seguridad que protege claves criptográficas y gestiona procesos de cifrado.
Beneficios: Garantiza la seguridad de firmas digitales, certificados y cifrado de datos sensibles.
Seguridad: Certificado bajo estándares internacionales como FIPS 140-2, asegurando máxima protección.
Redundancia: Configuración en clúster para asegurar disponibilidad continua de claves criptográficas.

Ambiente de KPI para grabado de chip de cédulas
Formado por un clúster en alta disponibilidad con componentes físicos y virtuales. Los cuales estarán compuestos por servidores redundantes.

Ambiente de KPI Ciudadana
Formado por un clúster en alta disponibilidad con componentes físicos y virtuales. Los cuales estarán compuestos por servidores redundantes:

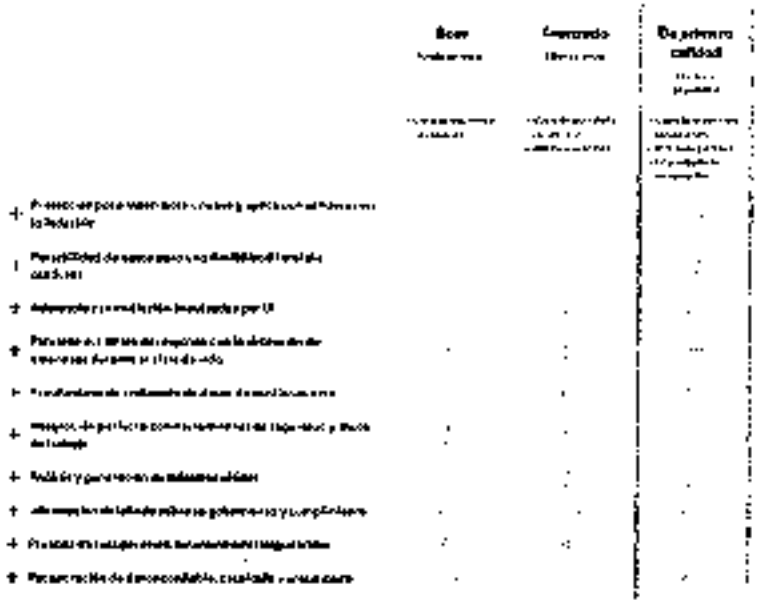
- PKI
- ACC RAIZ
- AC Subordinada
- Vertical de Firma
- SeguriSign, SeguriNotary, OCSP (Cloud)

Ambiente de Mobile ID
Formado por un clúster virtualizado formado por tres servidores en un ambiente totalmente en HA. Los cuales estarán compuestos por servidores virtuales redundantes:

- Database Server
- Authentication Server
- Application Server

Replicación y Orquestación

Para la replicación y orquestación del Site principal al Site alterno se incluye el licenciamiento de VEEAM Backup and Replicator en su versión Premium.



2. Plan de Trabajo Implementación Infraestructura en Centros de Datos

Este documento establece el plan de trabajo detallado para el proyecto del CLIENTE. El objetivo principal es actualizar y fortalecer la infraestructura tecnológica para mejorar la eficiencia operativa y garantizar un proceso de implementación, según las mejores prácticas del fabricante entregado por personal debidamente calificado y certificado.

2.1 Estructura del Plan de Trabajo

El proyecto se divide en varias fases, cada una con tareas y subtareas. Los recursos, las duraciones, las dependencias y las fechas de inicio y finalización se deben introducir en Microsoft Project.

2.2 Tareas y Alcances

Se incluyen los servicios de instalación e implementación de toda la solución propuesta.

2.2.1 Tareas Generales

- ✓ Nuestra propuesta incluye la asignación de un gerente de proyectos certificado PMP dedicado 100% de su tiempo a la implantación de todas las soluciones ofertadas hasta la conclusión y recepción del proyecto.

- ✓ Nuestra propuesta incluye plan de trabajo detallado en el cual se especifica de forma clara todos los pasos a ejecutar durante el proceso de implementación de la solución ofertada.
- ✓ Ejecución de pruebas.
- ✓ Documentación completa del proyecto.
- ✓ Capacitación del proceso de implementación.

2.2.2 Tareas de Implementación e Instalación

Servicio de implementación para el almacenamiento

- ✓ Instalación física del equipo
- ✓ Cableado del equipo
- ✓ Startup y configuración
- ✓ Actualización de versión de BIOS FIRMWARE y OS
- ✓ Creación de Raid Group y Volúmenes
- ✓ Pruebas de lectura y escritura

Tareas implementación Servidores

- ✓ Validación de Prerrequisitos de instalación
- ✓ Instalación física de servidores
- ✓ Configuración de out-of-band mgmt (iDRAC, CIMC, iLO, IMM, etc), arreglo de discos locales y políticas de BIOS.
- ✓ Instalación de sistema operativo.
- ✓ Ejecución de pruebas

Servicio de implementación Switches

- ✓ Validación de Prerrequisitos de instalación, incluyendo JCE
- ✓ Instalación de los Switches en Rack
- ✓ Encendido y Actualización de versión de UCSM, BIOS y Firmware
- ✓ Configuración de management y cluster
- ✓ Configuración de puertos para servidores
- ✓ Configuración de puertos y uplinks
- ✓ Integración a ambiente actual

Servicio de implementación VEEAM

- ✓ Validación de prerrequisitos de instalación
- ✓ Instalación y configuración básica VEEAM Backup
- ✓ Creación de Jobs de respaldo y Jobs de replicación

Servicio de implementación VMware

- ✓ Validación de Prerrequisitos de instalación, incluyendo JCE
- ✓ Instalación y configuración vCenter
- ✓ Instalación y configuración eSXI

Servicio de implementación Appliance Backup

- ✓ Validación de Prerrequisitos de instalación incluyendo JCE

- ✓ Instalación física del Appliance
- ✓ Configuración de networking
- ✓ Inicialización y configuración
- ✓ Configuración de proxy
- ✓ Pruebas de Backup/Respaldo

Consideraciones para el servicio

- ✓ La JCE debe proporcionar un área de trabajo adecuada para la entrega del servicio, incluido el acceso a una línea telefónica externa, energía y cualquier conexión de red requerida.
- ✓ La JCE debe permitir al Consorcio EMDOC acceso total y sin restricciones a todas las ubicaciones donde se realizará el servicio.

Premisas

- ✓ La capacidad del Consorcio EMDOC para brindar los servicios depende de la cooperación total y oportuna de la JCE con el Consorcio EMDOC, así como de la precisión e integridad de cualquier información y datos que la JCE proporcione al Consorcio EMDOC.
- ✓ Se incluyen en el proceso de entrega de los servicios varios recursos técnicos los cuales realizan la entrega de servicios en paralelo.
- ✓ La entrega programada de servicios se coordina entre el gerente de proyecto del Consorcio EMDOC y la JCE.

Entregables

- ✓ Capacitación.
- ✓ Documentación completa del proyecto.
- ✓ Pruebas funcionales y operativas.
- ✓ Reporte de certificación de trabajos concluidos, el cual incluye imágenes de los equipos ya instalados, y la confirmación de la puesta en servicio de la solución y/o equipo instalado.
- ✓ Certificación al final del proceso de implementación de que la misma fue realizada según las mejores prácticas y en cumplimientos de versiones de software recomendados al momento de la implementación

3. Justificación

3.1. Los equipos del Ambiente Productivo de la PKI y DRP se justifican de la siguiente manera:

SeguriServer (AC Raiz):

Recurso	Justificación
Procesador	La AC raíz ejecutará tareas críticas como la firma de certificados subordinados y listas de revocación (CRL). Un procesador con 10 núcleos es suficiente, ya que esta CA opera en un entorno aislado con baja carga transaccional, sin embargo, se conectará al

	Cryptoserver CP5 SE12, por lo cual requiere esta capacidad de procesamiento.
Memoria RAM	Se requiere una cantidad de RAM adecuada para ejecutar Windows Server 2022, gestionar firmas digitales y realizar auditorías de seguridad sin degradar el rendimiento.
Almacenamiento	Se utiliza almacenamiento NVMe SSD por su velocidad y confiabilidad Dado que la AC raiz solo firmará certificados en momentos específicos y la base de datos estará en un servidor externo, este espacio es suficiente para el sistema operativo, software PKI y logs de auditoría.
Sistema Operativo	Compatible con los requisitos de PKI, HSM UTIMACO y cumple con los lineamientos de seguridad y compatibilidad requeridos para la infraestructura.

SeguriServer (AC Ruiz)

Recurso	Justificación
Procesador	Se requiere un CPU con alto rendimiento en procesamiento paralelo para manejar la carga computacional de la generación y validación de claves criptográficas, firmas digitales y operaciones de cifrado/descifrado. Un procesador con múltiples núcleos permite optimizar la concurrencia de procesos y minimizar la latencia, lo que es fundamental al momento de crear los certificados de la PKI ciudadana. Adicionalmente, este servidor estará conectado al Cryptoserver CP5 SE 500, por lo cual requiere un mayor procesamiento para comunicarse de manera efectiva con el mismo.
Memoria RAM	La PKI debe manejar múltiples peticiones simultáneas, desde la emisión de certificados hasta su validación en tiempo real. Además, el entorno requiere ejecución eficiente de servicios de autenticación y cifrado, minimizando el riesgo de degradación del rendimiento.
Almacenamiento	Se opta por almacenamiento NVMe SSD debido a su velocidad de lectura/escritura superior, lo que mejora el tiempo de respuesta del sistema. Este espacio cubre el sistema operativo, aplicaciones y logs de auditoría. La base de datos de certificados se alojará en un servidor externo, optimizando la distribución de carga.
Sistema Operativo	Compatible con los requisitos de PKI y cumple con los lineamientos de seguridad y compatibilidad requeridos para la infraestructura.
	Portal de Firma
Recurso	Justificación
Procesador	Se requiere un procesador de alto rendimiento con múltiples núcleos para manejar la concurrencia de solicitudes en el portal y la ejecución de microservicios en Java. Los procesos de firma digital y cifrado demandan potencia computacional significativa, especialmente en cargas transaccionales altas.

Memoria RAM	Los microservicios en Java tienden a un alto consumo de memoria debido a la administración de sesiones, el manejo de documentos y las validaciones criptográficas. Se requiere suficiente RAM para evitar cuellos de botella y garantizar tiempos de respuesta óptimos.
Almacenamiento	Se opta por almacenamiento NVMe SSD debido a su velocidad superior, lo que reduce la latencia en la ejecución de servicios y el acceso a logs. Aunque la base de datos es externa, este espacio es necesario para almacenar logs de auditoría, archivos temporales y procesamiento de documentos.
Sistema Operativo	Se requiere un sistema operativo estable y seguro que sea compatible con Java, Apache Tomcat y la infraestructura de microservicios, garantizando compatibilidad con entornos empresariales.
	SeguriSign, SeguriNotary, OCSP
Recurso	Justificación
Procesador	Se requiere un procesador de alto rendimiento para gestionar múltiples solicitudes concurrentes de firma, validación y estampillado en tiempo real. Cada operación criptográfica consume recursos intensivos de CPU, especialmente en volúmenes altos de transacciones.
Memoria RAM	Los servicios de firma, TSA y OCSP requieren gestión eficiente de memoria, ya que manejan múltiples sesiones simultáneamente. Los microservicios en Java y los servidores Tomcat también incrementan el consumo de memoria.
Almacenamiento	Se utiliza almacenamiento NVMe SSD debido a su velocidad y confiabilidad. Aunque la base de datos es externa, este espacio es necesario para logs de auditoría, transacciones temporales y caché de validación OCSP.
Sistema Operativo	Se requiere un sistema operativo estable y seguro que sea compatible con Java, Apache Tomcat y la infraestructura de microservicios, garantizando compatibilidad con entornos empresariales.
	Base de Datos
Recurso	Justificación
Procesador	Se requiere una CPU de alto rendimiento debido al procesamiento intensivo de consultas, índices y transacciones. La base de datos manejará operaciones criptográficas, validaciones y logs de auditoría de los servicios core.
Memoria RAM	SQL Server realiza almacenamiento en caché de consultas y datos en memoria para optimizar tiempos de respuesta. Se requiere esta capacidad para soportar la carga transaccional y minimizar el acceso a disco.
Almacenamiento	Se utiliza NVMe SSD para garantizar tiempos de acceso ultrarápidos, minimizando la latencia en la escritura y lectura de datos. Se estima un almacenamiento eficiente para 4,000,000 de

	documentos en dos años, esto debido a la emisión de 800,000 certificados para ciudadanos y un promedio de 5 firmas de documentos por ciudadano. Tomando como consideración un peso promedio por PDF de 1.7 MB y un promedio de dos firmas por documento, queda un tamaño final de 2 MB por documento concluido. Tomando en consideración lo anterior, bajo el supuesto de que cada usuario firma 5 documentos por año, se tiene que en dos años se firmarán 4,000,000 de documentos multiplicado por los 2 MB, da un total de 8TB para la base de firma, a esto se debe aumentar las otras bases que utiliza la plataforma de firma y que, en promedio, por dos años medirán de 1 TB.
Sistema Operativo	Garantiza compatibilidad total con SQL Server 2022, con soporte para configuraciones avanzadas de clúster y alta disponibilidad.

4. Justificación del Plan de Recuperación y Respaldo

El Consorcio EMDOC con la finalidad de garantizar la continuidad del negocio y la recuperación ante desastres de la infraestructura PKI, propone el siguiente implementación de un plan integral de Disaster Recovery Plan (DRP) alineado con estándares internacionales como la ISO/IEC 27031, que establece directrices para la preparación en tecnologías de la información, y la ISO 22301, enfocada en sistemas de gestión de continuidad del negocio. Este plan no solo asegura el cumplimiento normativo, sino que también prioriza la disponibilidad y protección de los servicios críticos y la información sensible alojada en el Centro de Datos.

Como herramienta clave para la ejecución efectiva de este plan, estaremos utilizando Veeam Backup and Replication en su versión Premium. Esta solución permite gestionar de manera eficiente los respaldos y la replicación de datos, asegurando una recuperación rápida y confiable (Recovery Time Objective - RTO) ante incidentes que afecten la infraestructura o los servicios de la PKI. Veeam Backup and Replication Premium ofrece funcionalidades avanzadas para proteger, mitigar y gestionar riesgos y amenazas, ya sean de origen físico, lógico o por error humano. Entre sus capacidades destacan:

- **Respaldo y replicación automatizados**: Garantiza la integridad y disponibilidad de la información crítica mediante copias de seguridad consistentes y réplicas en tiempo real de los sistemas PKI.
- **Soporte Específico para Bases de Datos PostgreSQL y Microsoft SQL Server**: La capacidad de Veeam para manejar estas bases de datos asegura que los servicios críticos dependientes (como PKI, firma ciudadana y Mobile ID) puedan recuperarse de manera ordenada y funcional, respetando las mejores prácticas de la industria.
- **Recuperación granular y rápida**: Permite restaurar servicios o datos específicos en minutos, minimizando el impacto en las operaciones.
- **Gestión centralizada**: Facilita la administración de respaldos y réplicas, asegurando una visión integral de la infraestructura crítica.

- **Pruebas de recuperación:** Ofrece la posibilidad de simular escenarios de desastre sin afectar los entornos productivos, validando la efectividad del DRP.
- **Cumplimiento de políticas de continuidad:** Asegura que los tiempos de recuperación y la disponibilidad de datos cumplan con los objetivos estratégicos de la empresa.

Con Veeam Backup and Replication Premium, la empresa podrá proteger su infraestructura PKI frente a interrupciones no planificadas, garantizando la continuidad del negocio y la disponibilidad de servicios esenciales. Esta solución, combinada con un DRP bien estructurado, proporciona una respuesta proactiva y robusta ante cualquier eventualidad, salvaguardando tanto la operatividad como la información vital para el cumplimiento de los objetivos organizacionales.

Abordaje para recuperación ante desastres

A continuación, se detalla el enfoque recomendado para la recuperación manual (basado en recomendaciones de la industria y mejores prácticas), respetando el orden de encendido establecido:

1. Bases de datos, ambientes virtuales y aplicaciones secundarias:
a. Se iniciará la restauración manual de las bases de datos críticas, esenciales para el funcionamiento de los sistemas, utilizando las funcionalidades de recuperación granular de Veeam. Esto asegura que los datos estén disponibles antes de proceder con otros componentes.
b. Posteriormente, se restaurarán los ambientes virtuales que soportan estas bases y las aplicaciones secundarias, verificando su integridad y conectividad paso a paso, conforme a las mejores prácticas de recuperación de entornos virtualizados.
2. Ambiente PKI:
a. Una vez confirmado el funcionamiento de las bases de datos y los ambientes virtuales, se procederá con la recuperación manual del ambiente PKI. Veeam permite restaurar las máquinas y configuraciones específicas de este entorno, asegurando que los servicios de infraestructura de clave pública estén operativos antes de avanzar al siguiente nivel.
3. Ambiente de firma ciudadana y Mobile ID:
a. Finalmente, se restaurará el ambiente de firma ciudadana y Mobile ID, que depende de la disponibilidad previa del PKI y las aplicaciones secundarias. Este paso se ejecutará manualmente, validando cada componente para garantizar la continuidad de los servicios ciudadanos sin interrupciones.

Cabe destacar que se recomienda a la JCE realizar ejercicios de recuperación ante desastres para garantizar la ejecución optima de procesos y controles que garanticen una correcta operación luego del desastre en el sitio secundario. Estos ejercicios deben ser realizados por la JCE, con el apoyo del personal del Consorcio EMDOC

Recomendaciones para el Plan de Recuperación Ante Desastres

Basado en las normativas ISO/IEC 27031 (directrices para la preparación en tecnologías de la información) e ISO 22301 (sistemas de gestión de continuidad del negocio), las recomendaciones para los parámetros de RPO (Recovery Point Objective), RTO (Recovery Time Objective) y las pruebas dependen de la criticidad de los sistemas y

servicios involucrados, como la infraestructura PKI, las bases de datos, y los ambientes de firma ciudadana y Mobile ID. A continuación, se detallan las recomendaciones generales alineadas con estas normativas y adaptadas al contexto la plataforma ofertada, considerando las mejores prácticas de la industria y el uso de Veeam Backup and Replication Premium:

Componente	RPO Recomendado	RTO Recomendado	Frecuencia de Pruebas
Bases de datos y ambientes virtuales	15 min - 1 hora	1 - 4 horas	Trimestral + Anual
Ambiente PKI	15 min - 1 hora	4 - 8 horas	Trimestral + Anual
Firma ciudadana y Mobile ID	15 min - 1 hora	8 - 12 horas	Trimestral + Anual

Veeam Backup and Replication Premium ofrece una solución integral que satisface las necesidades técnicas y normativas de la JCE:

- Soporte avanzado para PostgreSQL y Microsoft SQL Server
- Flexibilidad para una recuperación manual ordenada
- Cumplimiento de RPO y RTO objetivos (15 min-1 hora y 1-12 horas, respectivamente)
- Capacidades de prueba robustas.

Protege la infraestructura crítica de la PKI y sus servicios asociados, asegurando la continuidad del negocio frente a cualquier incidente, mientras se alinea con las mejores prácticas y las normativas ISO/IEC 27031 e ISO 22301. Es una herramienta probada que combina eficacia, control y confiabilidad, lo que la convierte en la opción ideal para este caso.

5. Capacitación

Como parte de los entregables, se estarán realizando capacitaciones con el personal del Consorcio EMDOC en los que se habilitará a los ingenieros de la JCE en la correcta operación, mantenimiento y monitoreo de la infraestructura propuesta. A continuación se detallan estas capacitaciones.

5.1 Veeam Backup and Replication 12.1

La capacitación sobre Veeam Backup & Replication v12.1: Configuración, Gestión y Recuperación está diseñada para brindar a los participantes los conocimientos y habilidades necesarios para administrar y optimizar soluciones de respaldo y recuperación de datos utilizando Veeam. La capacitación se centra en la protección de datos en entornos físicos y virtuales desplegados en la JCE, incluyendo estrategias de seguridad, optimización del almacenamiento y recuperación ante desastres.

Metodología

El curso sigue una metodología teórico con ejemplos prácticos de lo implementado. Se utilizarán los siguientes métodos de enseñanza:

- ✓ Presentaciones teóricas: Explicaciones sobre cada tema clave.
- ✓ Ejemplos prácticos. Guía y muestra en vivo de la herramienta para reforzar conceptos basado en la configuración implementada.
- ✓ Preguntas y respuestas: Espacios interactivos para resolver dudas.
- ✓ Duración: dos (2) días.

Incluye:

- ✓ Conceptos clave de seguridad en Veeam.
- ✓ Visualización de la configuración y optimización de backups y réplicas.
- ✓ Gestión del almacenamiento y estrategias de recuperación.
- ✓ Pruebas de recuperación y validación de integridad.
- ✓ Escenarios prácticos con resolución de problemas.
- ✓ Certificado de participación provisto por el Consorcio EMDOC.
- ✓ Capacitación para cinco (5) Ingenieros de la JCE.
- ✓ La capacitación será impartida en las instalaciones de la JCE.

No Incluye:

- ✓ Implementaciones personalizadas.
- ✓ Configuración avanzada fuera del entorno estándar del curso.
- ✓ Material oficial, libros y/o guías de certificación.
- ✓ Refrigerio.
- ✓ Certificación oficial del fabricante.

5.1.1 Objetivos de la Capacitación

Al finalizar la capacitación, los participantes podrán:

1. Comprender las estrategias de protección de datos y mitigación de riesgos.
2. Configurar y gestionar trabajos de backup y copia de seguridad.
3. Implementar medidas de seguridad para proteger la infraestructura de respaldo.
4. Optimizar el almacenamiento mediante técnicas avanzadas de Veeam.
5. Restaurar datos utilizando diferentes métodos de recuperación.
6. Integrar Veeam en planes de respuesta ante incidentes.

5.1.2 Temario de la Capacitación

1. Introducción a la Protección de Datos
   - Importancia del respaldo y recuperación.
   - Estrategias clave de protección de datos.
2. Componentes Clave de Veeam Backup & Replication
   - Infraestructura básica.
   - Requisitos del sistema.
3. Visualización de configuración Inicial y Seguridad
   - Visualización de configuración del servidor de backup.
   - Medidas de seguridad para evitar accesos no autorizados.
4. Creación y Gestión de Backups
   - Respaldo de máquinas virtuales (VMware y Hyper-V).
   - Protección de datos no estructurados y agentes de backup.
5. Optimización del Almacenamiento y Retención
   - Técnicas de optimización de datos.
   - Repositorios de backup y almacenamiento en la nube.

6. Replicación y Alta Disponibilidad
   - Configuración de trabajos de replicación.
   - Protección continua de datos (CDP).
7. Recuperación de Datos y Planificación ante Incidentes
   - Métodos de recuperación según escenarios.
   - Integración de Veeam en planes de respuesta ante incidentes.

5.2 VMware vSphere: Operate, Scale and Secure

La capacitación VMware vSphere: Operate, Scale and Secure (V8) está diseñada para brindar conocimiento en la gestión avanzada de VMware vSphere 8. Se enfoca en la configuración, escalabilidad y seguridad de entornos virtualizados, cubriendo desde la administración de redes y almacenamiento hasta la protección y recuperación de máquinas virtuales.

Metodología
Esta capacitación tiene un enfoque teórico con ejemplos prácticos. Se utilizarán los siguientes métodos de enseñanza:

- ✓ Presentaciones teóricas: Explicación de conceptos clave y mejores prácticas.
- ✓ Ejemplos prácticos: Guía y muestra en vivo en el ambiente real de VMware vSphere para reforzar el aprendizaje.
- ✓ Espacios de preguntas y respuestas: Interacción para aclarar dudas.
- ✓ Duración: dos (2) días.

Incluye:

- ✓ Conceptos clave de VMware vSphere 8.
- ✓ Gestión de seguridad, acceso y monitoreo de entornos virtualizados.
- ✓ Administración de alta disponibilidad y recuperación de máquinas virtuales.
- ✓ Estrategias de escalabilidad y optimización del rendimiento.
- ✓ Escenarios prácticos con resolución de problemas.
- ✓ Certificado de participación provisto por el Consorcio EMDOC.
- ✓ Capacitación para cinco (5) ingenieros de la JCE.
- ✓ La capacitación será impartida en las instalaciones de la JCE.

No Incluye:

- ✓ Implementaciones personalizadas.
- ✓ Configuración avanzada fuera del entorno estándar del curso.
- ✓ Material oficial, libros y/o guías de certificación.
- ✓ Refrigerio.
- ✓ Certificación oficial del fabricante.

5.2.1 Objetivos de la Capacitación

Al finalizar la capacitación, los participantes podrán:

1. Administrar un VMware Tools Repository.

2. Operar vSphere Replication y recuperar máquinas virtuales replicadas.
3. Gestionar recursos de máquinas virtuales mediante Resource Pools.
4. Administrar redes y almacenamiento para entornos empresariales complejos.
5. Implementar alta disponibilidad en VMware vCenter Server.
6. Monitorear el rendimiento de vCenter, ESXi y máquinas virtuales.

5.2.2 Temario de la Capacitación

1. Introducción al Curso
2. Operaciones con Máquinas Virtuales
   - Administración de VMware Tools Repository.
   - Soluciones de respaldo y restauración de VMs.
   - Visualización de configuración de vSphere Replication y Site Recovery.
3. Gestión de Clústeres en vSphere
   - Visualización y administración de Resource Pools.
   - Funcionamiento de vCLS (vSphere Cluster Services).
4. Administración de vCenter y ESXi
   - Programación de respaldos de vCenter.
   - Visualización de alta disponibilidad en vCenter.
   - Uso de Host Profiles para la gestión de ESXi.
5. Monitoreo en vSphere
   - Factores clave que afectan el rendimiento de VMs.
   - Uso de herramientas de vCenter para análisis de recursos.
6. Seguridad y Control de Acceso
   - Estrategias de seguridad en vCenter, ESXi y VMs.

5.3 HPE ProLiant Gen11 Server Management with iLO 6

La capacitación de HPE ProLiant Gen11 Server Management with iLO 6 está diseñado para administradores e ingenieros que necesitan aprender a configurar, actualizar, monitorear y gestionar servidores HPE ProLiant Gen11 utilizando herramientas de administración embebidas como Integrated Lights-Out (iLO) 6.

Esta capacitación cubre desde la configuración inicial del hardware hasta la supervisión avanzada y actualización del firmware, proporcionando un enfoque integral para la gestión eficiente de servidores HPE en entornos empresariales.

Metodología
La capacitación combina teoría con ejemplos prácticos en un entorno real. Se utilizan los siguientes métodos de enseñanza:

- ✓ Presentaciones teóricas: Explicación detallada de conceptos clave.
- ✓ Ejemplos prácticos: Guía y muestra en vivo de servidores y herramientas en tiempo real.
- ✓ Interacción en sesiones de preguntas y respuestas
- ✓ Duración: un (1) día.

Incluye:

- ✓ Administración de servidores HPE ProLiant Gen11.
- ✓ Gestión de iLO 6 para monitoreo y administración remota.
- ✓ Métodos para actualización de firmware con SPP y SUM.
- ✓ Visualización de configuración de seguridad, rendimiento y energía.
- ✓ Certificado de participación provisto por el Consorcio EMDOC.
- ✓ Capacitación para cinco (5) ingenieros de la JCE.
- ✓ La capacitación será impartida en las instalaciones de la JCE.

No Incluye:

- ✓ Implementaciones personalizadas.
- ✓ Configuración avanzada fuera del entorno estándar del curso.
- ✓ Material oficial, libros y/o guías de certificación.
- ✓ Refrigerio.
- ✓ Certificación oficial del fabricante.

5.3.1 Objetivos de la Capacitación

Al finalizar el curso, los participantes serán capaces de:

1. Diferenciar las características de los servidores HPE ProLiant Gen11 y sus opciones de hardware y software.
2. Operar herramientas de administración embebida como iLO 6, UEFI ROM, y Intelligent Provisioning.
3. Visualizar medidas de seguridad y monitoreo para optimizar el rendimiento y consumo energético.
4. Monitorear servidores utilizando la interfaz de iLO 6, comandos REST y herramientas en la nube.
5. Actualizar el firmware de los servidores utilizando Service Pack for ProLiant (SPP) y Smart Update Manager (SUM).
6. Diagnosticar y solucionar problemas utilizando herramientas como Active Health System (AHS) y UEFI Embedded Diagnostics.

5.3.2 Temario de la Capacitación

1. Introducción al Hardware de HPE ProLiant Gen11
   - Características de los servidores Gen11.
   - Opciones de hardware y software.
   - Seguridad, garantía y soporte.
2. Introducción a las Herramientas de Administración
   - Gestión embebida en HPE ProLiant.
   - Uso de iLO 6, UEFI ROM, Intelligent Provisioning y Active Health System.
   - Gestión basada en la nube y Baseboard Management Controller (BMC).
3. Administración con iLO 6
   - Acceso remoto y administración de servidores.
   - Configuración de seguridad y políticas de acceso.
   - Opciones de gestión de energía y temperatura.
4. Actualización del Servidor
   - Métodos de actualización de firmware.

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

- Uso de Service Pack for ProLiant (SPP) y Smart Update Manager (SUM).
- Procedimientos de actualización de iLO 6.

5. Monitoreo del Servidor
   - Uso de iLO 6 y herramientas de monitoreo.
   - Configuración de alertas y análisis de rendimiento.
   - Verificación de firmware y monitoreo con RESTful API.
6. Diagnóstico y Solución de Problemas
   - Herramientas de diagnóstico embebidas en UEFI e iLO.
   - Descarga y análisis de logs con Active Health System (AHS).
   - Indicadores LED y su interpretación.
7. Recursos y Soporte
   - Uso del HPE Support Center y My Software Center Dashboard.
   - Acceso a actualizaciones y materiales de soporte.
   - Pasos siguientes para continuar el aprendizaje.

6. Premisas y Entregables

- ✓ El Consorcio EMDOC se hace responsable de la entrega de todos los servicios de instalación y configuración de los equipos ofertados.
- ✓ El Consorcio EMDOC se hace responsable de la realización de las configuraciones, actualizaciones y mejoras de software necesarias para la integración de los nuevos equipos.
- ✓ Nuestra propuesta incluye todo el hardware, software y licenciamientos necesarios para la instalación y operación tal y como es requerido.
- ✓ Nuestra propuesta incluye soporte de tipo proactivo con SLA de atención 24x7x4 con una duración de cinco (5) años a partir de la fecha de aceptación por escrito por parte de la Junta Central Electoral y puesta en marcha de los equipos.
- ✓ Nuestra propuesta incluye equipos nuevos no reconstruidos.
- ✓ Nuestra propuesta incluye plan de trabajo detallado en la propuesta técnica en el cual se especifica de forma clara todos los pasos a ejecutar durante el proceso de implementación de los equipos ofertados.
- ✓ Nuestra propuesta incluye proveer, instalar y configurar todos los equipos, hardware y licencias con las características técnicas mencionadas según la tabla de referencias. La solución propuesta está integrada y certificada de fábrica en todos sus componentes como un solo producto según cada lote.
- ✓ Nuestra propuesta incluye la entrega de todos los equipos en completa operación, a satisfacción de la entidad, con todos los componentes solicitados incluidos.
- ✓ Se incluyen todas las hojas técnicas (DataSheets) de los propuestos ofertados, así como el link correspondiente del fabricante.
- ✓ Nuestra propuesta incluye equipos nuevos de fábrica, no se incluyen equipos reemplazos o remanufacturados.
- ✓ Se incluyen cartas del fabricante en la cual el Consorcio EMDOC a través de los miembros del consorcio cuenta con las debidas autorizaciones a ofrecer los bienes y servicios presentados en nuestra oferta.

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

- ✓ Se incluye carta del fabricante en la cual se indica que todos los equipos ofertados son nuevos, no usados, no remanufactorados, ni reparados y que los mismos no se encuentran descontinuados ni anunciados fuera de vida.
- ✓ Nuestra propuesta incluye la asignación de un gerente de proyectos certificado PMP dedicado 100% de su tiempo a la implantación de todas las soluciones ofertadas en este lote durante todo el tiempo que sea necesario y requerido por la institución hasta la conclusión y recepción del proyecto. Este Gerente de proyecto es empleado fijo de uno de los miembros del Consorcio EMDOC con más de 6 meses en la empresa.

EMDOC
CONSORCIO

SECCIÓN VII. CAPACITACIÓN

PARA LA CONTRATACIÓN DE LA EMPRESA QUE SE ENCARGARÁ DE SUPLIR LOS EQUIPOS, MATERIALES Y SERVICIOS PARA LA IMPRESIÓN DE LA CÉDULA DE IDENTIDAD Y ELECTORAL (CIE) Y CÉDULA DE IDENTIDAD (CI)

CONSORCIO EMDOC
EMDOC CONSORCIO
Santo Domingo, RD

EMDOC

Tabla de contenido

1. *Plan de Capacitación* 3
2. *Metodología* 4
3. *Planificación para las Capacitaciones* 4
4. *Temario de Capacitaciones Básicas:* 5
   - 4.1. Capacitación del uso de las impresoras de cédulas 5
   - 4.2. Capacitación del mantenimiento básico de la máquina de impresión 5
   - 4.3. Introducción de la Cédula Digital 6
5. *Temario de Capacitaciones Avanzadas:* 6
   - 5.1. Capacitación para el uso, Administración y Mantenimiento de la PKI Grabado de Chip: 6
   - 5.2. *Capacitación del uso, administración y Mantenimiento de la PKI CA* 7
   - 5.3. Capacitación para el uso, administración y mantenimiento de las impresoras 7
   - 5.4. Capacitación de Uso, administración y mantenimiento de la cédula digital (app y web). 8
     - 5.4.1. Plan de formación: Operaciones y configuración de un monedero de identificación ISO 18013-5 basado en Linux y aplicaciones de verificación utilizando Docker Pods 8
   - 5.5. Uso, administración y mantenimiento de los dispositivos. 12
     - 5.5.1. Capacitación en mantenimiento de máquina de impresión 12
     - 5.5.2. Capacitación de Centro de Datos 12
     - 5.5.3. Veeam Backup and Replication 12.1 13
       - Objetivos de la Capacitación 13
       - Temario de la Capacitación 13
     - 5.5.4. Capacitación VMware vSphere: Operate, Scale and Secure 14
       - Objetivos de la Capacitación 15
       - Temario de la Capacitación 15
     - 5.5.5. Capacitación HPE ProLiant Gen11 Server Management with iLO 6 16
     - 5.5.6. Objetivos de la Capacitación 16
       - Temario de la Capacitación 17
6. *Premisas y Entregables* 19

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

EMDOC
CONSORCIO

1. Plan de Capacitación

El Consorcio EMDOC deberá presentar un plan de capacitación completo. El cual incluirá todos los aspectos técnicos:

1- El plan de Capacitación cubre todos los aspectos técnicos de la puesta en marcha del presente contrato.
2- El plan de capacitación todos los productos y servicios incluidos en su oferta.
3- El plan de capacitación debe incluir una capacitación al personal que gestionará las máquinas.

El Consorcio EMDOC brindará un (1) curso al año solamente durante los dos (2) años iniciales del proyecto y en todo caso presenciales.

En el pliego de condiciones específicas la JCE indicó que para la parte de la Direcion Nacional de Cedulación, Dirección Ejecutiva del Voto Dominicano en el Exterior y Centros de Expediciones de Actas y Cédulas son 436 empleados divididos como sigue: 370 local y 66 en el exterior, además de 50 técnicos del equipo de tecnología.

El Consorcio EMDOC capacitará al personal de la JCE (a capacitadores de la JCE, donde será la JCE encargada de capacitar al resto de personal de la entidad) en la sede central de la JCE, en los siguientes cursos (1 curso por año de cada curso):

1- Uso, administración y mantenimiento de la PKI.
2- Uso, administración y mantenimiento de las impresoras.
3- Uso, administración y mantenimiento de la cédula digital (app y web).
4- Uso, administración y mantenimiento de los dispositivos.
5- Uso, administración y mantenimiento de los API's.

El Consorcio EMDOC brinda en esta propuesta cómo impartirá la capacitación en su oferta.

Este plan incluye todos los productos y servicios especificados en esta oferta, así como la capacitación del personal encargado de gestionar los equipos, sistemas y componentes que integren la solución propuesta por el oferente.

En este sentido, en conformidad con lo requerido, la capacitación debe ser integral y detallada, abarcando, como mínimo, los siguientes aspectos:

Niveles de Capacitación:

1- **Básico**: Capacitación destinada al personal operativo que realizará tareas cotidianas relacionadas con el manejo de los equipos de impresión y las aplicaciones asociadas.
2- **Avanzado:** Capacitación para el personal técnico y administrativo que supervisará, mantendrá y resolverá problemas complejos relacionados con la infraestructura de PKI, CA, y la solución de Mobile ID.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

1. **Operación y Mantenimiento del Equipo de Impresión:**

a. Instalación y configuración de impresoras de policarbonato.
b. Procedimientos de personalización de tarjetas.
c. Mantenimiento preventivo y correctivo de los equipos.

2. **Infraestructura de Clave Pública (PKI) y Autoridad de Certificación (CA):**

a. Principios básicos de PKI y su aplicación en documentos de identidad.
b. Generación, manejo y almacenamiento seguro de claves criptográficas.
c. Procedimientos para la emisión y revocación de certificados digitales.
d. Uso y gestión de Módulos de Seguridad por Hardware (HSM).

3. **Solución de Mobile ID:**

a. Funcionamiento y uso de la app de Mobile ID desarrollada para la JCE.
b. Procedimientos de seguridad para la gestión de identidades digitales.
c. Integración con sistemas existentes y gestión de actualizaciones.

2. Metodología

Para la capacitación el personal de la JCE, operativo, técnico y administrativo, se utilizará la siguiente metodología:

1. Estrategia: Se establecerá una estrategia de trabajo con el personal, y se realizará una presentación audiovisual, durante el proceso de transferencia de conocimiento y entrenamiento del personal. A su vez se brindarán documentos de guía de la capacitación para respaldar los contenidos mostrados.
2. Orientación teórica: La cual permita brindar a todos los participantes de los mismos términos.
3. Evaluación de competencias: Se brindan los perfiles del personal a participar de este plan, con la intención de asegurarnos que la misma será viable para la ejecución del proyecto.
4. Orientación práctica: Guía y muestra en vivo de la herramienta para reforzar conceptos, en donde los participantes podrán poner en ejecución los conocimientos técnicos.
5. Preguntas y respuestas: Espacios interactivos para resolver dudas.

3. Planificación para las Capacitaciones

Para las capacitaciones, se contempla realizar las siguientes actividades para la Planificación de la Capacitación, de acuerdo a la siguiente tabla:

1. Validación de Requerimientos para la Capacitación entre la JCE y el Consorcio EMDOC.
2. Actividades de logística del Consorcio EMDOC para la capacitación.
3. Manuales y documentación para la capacitación que brindará el Consorcio EMDOC.
4. Preparación de Certificados de Capacitación.

Se atenderán según la planificación que se realice con la JCE.

4. Temario de Capacitaciones Básicas:

Se brinderán las siguientes capacitaciones básicas al personal operativo de las localidades de la JCE:

4.1. Capacitación del uso de las impresoras de cédulas

Se capacitará al personal de la JCE en la operación y manejo de las impresoras de cédulas:

1. Presentación de la máquina de impresión.
2. Operación y manejo de la máquina de impresión.
3. Manejo de excepciones de la máquina de impresión en la operación.
4. Prácticas en el uso de la máquina de impresión.

Se recomienda que el personal de la JCE que reciba la capacitación posea este perfil:

- Personal con conocimientos básicos de computación.
- Conocimientos básicos en operación de periféricos de computación.
- Conocimiento en manejo de software de impresión (recomendado)

4.2. Capacitación del mantenimiento básico de la máquina de impresión

Se capacitará al personal de la JCE en la operación y manejo de la máquina de impresión:

1. Presentación de la máquina de impresión.
2. Operación y manejo de la máquina de impresión.
3. Mantenimiento básico de la máquina de impresión.
4. Manejo de excepciones de la máquina de impresión en la operación.
5. Prácticas en el uso de la máquina de impresión.
6. Materiales de limpieza y cuidados de la máquina de impresión.

Se recomienda que el personal de la JCE que reciba la capacitación posea este perfil:

- Personal con conocimiento básicos de computación.
- Conocimientos básicos en operación de periféricos de computación.
- Conocimiento en manejo de software de impresión (recomendado)

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

4.3. Introducción de la Cédula Digital

Se capacitará al personal de la JCE en la operación y manejo de la máquina de impresión:

1. Presentación de la cédula digital.
2. Condiciones requeridas para su descarga e instalación.
3. Guía de la instalación.

Se recomienda que el personal de la JCE que reciba la capacitación posea este perfil:

- Personal con experiencia en uso de dispositivos móviles.
- Conocimiento en manejo de navegadores web.

5. Temario de Capacitaciones Avanzadas:

5.1. Capacitación para el uso, Administración y Mantenimiento de la PKI Grabado de Chip:

Se capacitará al personal de la JCE en el manejo y la resolución de problemas del sistema PKI suministrado. Esta formación abarcará los siguientes temas.

1. Administración y supervisión de la PKI y sus componentes de hardware y software,
2. Fundamentos de la criptografía.
3. Introducción a la criptografía moderna.
4. Aspectos tecnológicos y organizativos básicos de la PKI.
5. Estructura específica de un documento de viaje electrónico legible por máquina PKI.
6. Estructura específica de una PKI X.509 de propósito general.
7. Introducción a Veridos Certificate Manager (ICAO PKI).
8. Introducción a Veridos Starfish PKI (PKI de firma).
9. Procesos empresariales que se realizarán en los sistemas PKI.
10. Introducción a la interfaz de usuario de los sistemas PKI.
11. Gestión del OCSP Responder en la nube.
12. Solución de problemas.

Se facilitará la documentación adecuada para la formación. Los aspectos organizativos, como la provisión de salas y equipos adecuados, son responsabilidad del cliente.

Se recomienda que el personal de la JCE que reciba la capacitación posea este perfil:

1. Especialistas en TI con conocimientos básicos de criptografía y operación de PKI (recomendado)
2. Conocimientos básicos sobre la configuración de PKI (recomendado)
3. Conocimientos básicos de Autoridades de certificación
4. Formatos de la base de datos
5. Conocimiento avanzado de los servicios de directorio LDAP (recomendado)

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

6. Conocimientos avanzados de bases de datos (recomendado)
7. Conocimientos básicos de Java (recomendado)
8. Experiencia de configuración básica de Apache Tomcat (recomendada)

5.2. Capacitación del uso, administración y Mantenimiento de la PKI CA

Se capacitará al personal de la JCE en el manejo y la resolución de problemas del sistema PKI CA suministrado. Esta formación abarcará los siguientes temas.

1. CTPKI: Conceptos de seguridad aplicativa y sus elementos técnicos.
2. CTSER: SeguriServer - Conceptos, Administración y Operación de la Autoridad Certificadora Raiz/Subordinada y sus componentes.
3. CTSSIGN: SeguriSign - Conceptos, Administración y Operación de aplicaciones de Firma y sus componentes.
4. CTSNOTARY: SeguriNotary - Conceptos, Administración y Operación de Autoridad Emisora de Sellos de Tiempo
5. CDCB Conceptos Básicos de Integración y Estándares Criptográficos.
6. CDSGN SeguriSign Integración de los componentes de firma electrónica o digital.
7. CDSTSP SeguriNotary Integración de los componentes de la Autoridad Emisora de estampas de tiempo.
8. CDPFE Portal de Firma Electrónica Integración de los componentes de Web Services de Portal de firma electrónica.

Se recomienda que el personal de la JCE que reciba la capacitación corresponda a :

A. Responsables del área técnica que realizan la administración y operación de una Infraestructura de Llave Pública. Cuya tarea es asegurar la operación de la autoridad certificadora, el servidor de estampillas de tiempo, y los servicios de firma digital, gestión y autenticación de firmas digitales o electrónicas.

5.3. Capacitación para el uso, administración y mantenimiento de las impresoras.

Se capacitará al personal de la JCE en el manejo y la resolución de problemas del sistema PKI CA suministrado. Esta formación abarcará los siguientes temas:

1. **Capacitación para la instalación de la máquina de impresión:**

- Instalación física de las máquina de impresión de impresión
- Configuración del proceso de personalización / flujo de trabajo

Integración de software

- Integración con sistemas de terceros (por ejemplo, PKI, sistema JCE)

Gestión de usuarios

- Administración de las funciones adicionales introducidas para el sistema

Document Signer y KMS

CONSORCIO EMDOC SANTO DOMINGO RD

- Introducción a Document Signer y KMS (funcionalidad, estructura, componentes)
- Administración: introducción y renovación de certificados para el sistema PKI.

Se recomienda que el personal de la JCE posea los siguientes conocimientos:

- Ingenieros mecánicos
- Experiencia previa en la administración de entornos TIC complejos
- Experiencia previa en el mantenimiento y reparación mecánica y eléctrica en un entorno de fabricación industrial / automatizado.
- Preferiblemente licenciado en Ingeniería Mecánica (construcción) o Electrónica / Eléctrica.
- Se valorarán los conocimientos de inglés

2. **Capacitación en mantenimiento de máquina de impresión**

- Mantenimiento y reparación de componentes mecánicos
- Mantenimiento y reparación de componentes eléctricos y electrónicos

Se recomienda que el personal de la JCE posea los siguientes conocimientos:

- Ingeniero de máquina de impresión
- Conocimientos electrónicos necesarios (mecatrónica)
- Es necesario un ajuste mecánico básico
- Experiencia en máquina de impresión de alta tecnología
- Experiencia previa en la administración de sistemas informáticos.

Apoyo al personal operativo para resolver problemas técnicos

5.4. Capacitación de Uso, administración y mantenimiento de la cédula digital (app y web).

Se capacitará al personal de la JCE, en el manejo y la resolución de problemas del sistema Cédula Digital, app y web. Esta formación abarcará los siguientes temas:

5.4.1. Plan de formación: Operaciones y configuración de un monedero de identificación ISO 18013-5 basado en Linux y aplicaciones de verificación utilizando Docker Pods

A. Introducción

- **Objetivo:** Formar a los participantes en la configuración y el funcionamiento de una aplicación de billetera y verificador de identidad con certificación ISO 18013-5 deloyed on premise utilizando microservicios basados en Docker.

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

- **Destinatarios**: Administradores de sistemas, ingenieros DevOps, profesionales de la seguridad y formadores.
- **Metodología de formación**: Enfoque de formación de formadores para garantizar la escalabilidad de la transferencia de conocimientos.

B. Requisitos previos

- **Experiencia técnica**: Administración básica de Linux, fundamentos de Docker y arquitectura de microservicios.
- **Software necesario**:
  - Sistema operativo basado en Linux (se recomienda Ubuntu, CentOS o Debian)
  - Docker y Docker Compose
  - Kubernetes (opcional, para escalado)
  - Cartera de identificación y software verificador compatibles con ISO 18013-5
  - Redes y herramientas de seguridad (por ejemplo, OpenSSL, cortafuegos, VPN)

C. Módulos de formación

Módulo 1: Entender la norma ISO 18013-5 Carteras de identificación digital y aplicaciones verificadoras

- Visión general de la norma ISO 18013-5
- Ecosistema de identificación digital y modelos de confianza
- Autenticación y verificación de flujos de trabajo

Módulo 2: Linux y preparación del sistema

- Configuración del entorno Linux
- Gestión de usuarios y mejores prácticas de seguridad
- Configuraciones de red para microservicios

Módulo 3: Docker y arquitectura de microservicios

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

EMDOC

- Introducción a los contenedores y pods de Docker
- Configuración de Docker Compose para microservicios
- Gestión eficaz de contenedores Docker

Módulo 4: Implantación y configuración de las aplicaciones ID Wallet y Verifier

- Instalación y configuración del monedero y el verificador de documentos de identidad
- Protección de los microservicios mediante TLS/SSL
- Variables de entorno y configuraciones en tiempo de ejecución

Módulo 5: Pruebas y resolución de problemas

- Ejecución de pruebas funcionales en las aplicaciones de verificador y monedero
- Depuración de problemas habituales de implantación
- Registro y supervisión de microservicios

Módulo 6: Buenas prácticas para la formación de formadores

- Estructuración de las sesiones de transferencia de conocimientos
- Creación de documentación y guías de usuario
- Demostraciones prácticas y organización de talleres

D. Ejercicios Prácticos:

Se contará con 4 ejercicios de laboratorio para la capacitación inicial en donde se brindarán ejercicios prácticos para los participantes de la JCE, tal como se detalla a continuación:

1. **Laboratorio 1**: Despliegue de un monedero y verificador de identidad en contenedores.
2. **Laboratorio 2**: Configuración de SSL/TLS para una comunicación segura
3. **Laboratorio 3**: Resolución de problemas comunes en la implantación.
4. **Laboratorio 4**: Impartir una sesión de formación simulada.

Se espera que el personal de la JCE cumpla con lo siguiente:

CONSORCIO EMDOC Santo Domingo R.D.

EMDOC

1. Visión general de alto nivel: Programa de formación de formadores

El programa de capacitación de formadores está diseñado para dotar a los formadores internos o externos de la experiencia y las habilidades necesarias para enseñar a los usuarios finales o a los miembros del equipo a utilizar eficazmente un producto de software. Al garantizar que los formadores tengan un conocimiento profundo del software y de las mejores prácticas para impartir una instrucción impactante, este programa crea un enfoque escalable y sostenible para la transferencia de conocimientos en toda la organización. El programa se centra en dos áreas críticas: dotar a los formadores de un dominio técnico del producto y desarrollar sus capacidades de instrucción para enseñar a públicos diversos.

2. Dominio del producto informático

La base del programa es proporcionar a los formadores un profundo conocimiento técnico del software. Se enseña a los formadores a navegar por todas las características y funciones, desde las operaciones básicas hasta los casos de uso avanzados, garantizando que estén equipados para manejar una amplia gama de necesidades de los usuarios. Esto incluye habilidades prácticas para solucionar problemas y responder a las preguntas más frecuentes, preparando a los formadores para ofrecer soluciones inmediatas a los problemas más comunes de los usuarios. Los formadores también adquieren conocimientos sobre la hoja de ruta de los productos de software, lo que les permite anticiparse a las futuras actualizaciones y comunicarlas de forma eficaz. Esto garantiza que el programa de formación evolucione en consonancia con el ciclo de vida del software, manteniendo tanto a los formadores como a los usuarios al día de las últimas funciones y mejoras.

3. Desarrollar habilidades docentes eficaces

Más allá de los conocimientos técnicos, el programa hace hincapié en el desarrollo de técnicas pedagógicas adaptadas a una amplia variedad de estilos de aprendizaje. Los formadores aprenden a simplificar conceptos técnicos complejos en lecciones claras y digeribles que resuenen en públicos diversos, desde principiantes a usuarios avanzados. El programa prioriza el uso de escenarios reales, enseñando a los formadores a demostrar el valor del software a través de aplicaciones prácticas. Se incorporan técnicas de enseñanza interactivas, como simulaciones, juegos de rol y ejercicios prácticos, para fomentar el aprendizaje activo y el compromiso, garantizando que los participantes retengan los conocimientos y se sientan seguros utilizando el software en sus funciones.

4. Recepción del Creación de material de formación

Para apoyar una impartición eficaz, el programa incluye el desarrollo de materiales de formación de alta calidad adaptados a diferentes contextos de aprendizaje. Los formadores disponen de un amplio conjunto de recursos, como presentaciones de diapositivas personalizables, guías de usuario detalladas, tutoriales paso a paso y preguntas frecuentes. Se crean videotutoriales y guías de software para ofrecer demostraciones visuales y mejorar la experiencia de formación de quienes prefieren

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

aprender a su propio ritmo o necesitan apoyo continuo. Además, se ofrecen ayudas de trabajo concisas, como hojas de trucos y guías de referencia rápida, para garantizar que los formadores y los usuarios finales tengan fácil acceso a la información esencial cuando la necesiten.

5. Impacto y escalabilidad del programa

El enfoque de Formación de Formadores garantiza que los conocimientos técnicos y la experiencia docente se distribuyan eficazmente dentro de la organización. Al invertir en un grupo básico de formadores, el programa crea un efecto dominó, en el que las personas formadas pueden transferir sus conocimientos a equipos o grupos de usuarios más amplios, reduciendo la dependencia de la asistencia externa. Este enfoque no sólo acelera la adopción del software, sino que también garantiza la coherencia de los mensajes, minimiza el tiempo de incorporación y mejora la satisfacción del usuario.

6. Marco de formación preparada para el futuro

Con la capacidad de adaptarse a las actualizaciones del producto y a las necesidades de la organización, el programa Train the Trainer proporciona un marco de formación preparado para el futuro. Los formadores se mantienen informados de los cambios en el software y ajustan sus contenidos de formación en consecuencia, garantizando la relevancia del programa a largo plazo. Esta inversión estratégica tanto en el conocimiento del producto como en la experiencia docente establece una base sólida para el uso generalizado y eficaz del software en toda la organización.

5.5. Uso, administración y mantenimiento de los dispositivos.

5.5.1. Capacitación en mantenimiento de máquina de Impresión

- Mantenimiento y reparación de componentes mecánicos
- Mantenimiento y reparación de componentes eléctricos y electrónicos

Se recomienda que el personal de la JCE posea los siguientes conocimientos:

- Ingeniero de máquina de impresión
- Conocimientos electrónicos necesarios (mecatrónica)
- Es necesario un ajuste mecánico básico
- Experiencia en máquina de impresión de alta tecnología
- Experiencia previa en la administración de sistemas informáticos.

5.5.2. Capacitación de Centro de Datos

Como parte de los entregables, se estarán realizando capacitaciones con el personal del Consorcio EMDOC en los que se habilitará a los ingenieros de la JCE en la correcta

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

operación, mantenimiento y monitoreo de la infraestructura propuesta. A continuación, se detallan estas capacitaciones:

5.5.3. Veeam Backup and Replication 12.1

La capacitación sobre Veeam Backup & Replication v12.1: Configuración, Gestión y Recuperación está diseñada para brindar a los participantes los conocimientos y habilidades necesarios para administrar y optimizar soluciones de respaldo y recuperación de datos utilizando Veeam. La capacitación se centra en la protección de datos en entornos físicos y virtuales desplegados en la JCE, incluyendo estrategias de seguridad, optimización del almacenamiento y recuperación ante desastres.

Metodología
El curso sigue una metodología teórica con ejemplos prácticos de lo implementado. Se utilizarán los siguientes métodos de enseñanza:

1- Presentaciones teóricas: Explicaciones sobre cada tema clave.
2- Ejemplos prácticos: Guía y muestra en vivo de la herramienta para reforzar conceptos basado en la configuración implementada.
3- Preguntas y respuestas: Espacios interactivos para resolver dudas.
4- Duración: dos (2) días.

Incluye:

1- Conceptos clave de seguridad en Veeam.
2- Visualización de la configuración y optimización de backups y réplicas.
3- Gestión del almacenamiento y estrategias de recuperación.
4- Pruebas de recuperación y validación de integridad.
5- Escenarios prácticos con resolución de problemas.
6- Certificado de participación provisto por el Consorcio EMDOC.
7- Capacitación para cinco (5) ingenieros de la JCE.
8- La capacitación será impartida en las instalaciones de la JCE.

Objetivos de la Capacitación

Al finalizar la capacitación, los participantes podrán:

1. Comprender las estrategias de protección de datos y mitigación de riesgos.
2. Configurar y gestionar trabajos de backup y copia de seguridad.
3. Implementar medidas de seguridad para proteger la infraestructura de respaldo.
4. Optimizar el almacenamiento mediante técnicas avanzadas de Veeam.
5. Restaurar datos utilizando diferentes métodos de recuperación
6. Integrar Veeam en planes de respuesta ante incidentes.

Temario de la Capacitación

1. Introducción a la Protección de Datos
   - Importancia del respaldo y recuperación.

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

- Estrategias clave de protección de datos.

2. Componentes Clave de Veeam Backup & Replication
   - Infraestructura básica.
   - Requisitos del sistema.
3. Visualización de configuración Inicial y Seguridad
   - Visualización de configuración del servidor de backup.
   - Medidas de seguridad para evitar accesos no autorizados.
4. Creación y Gestión de Backups
   - Respaldo de máquinas virtuales (VMware y Hyper-V).
   - Protección de datos no estructurados y agentes de backup.
5. Optimización del Almacenamiento y Retención
   - Técnicas de optimización de datos.
   - Repositorios de backup y almacenamiento en la nube.
6. Replicación y Alta Disponibilidad
   - Configuración de trabajos de replicación.
   - Protección continua de datos (CDP).
7. Recuperación de Datos y Planificación ante Incidentes
   - Métodos de recuperación según escenarios.
   - Integración de Veeam en planes de respuesta ante incidentes.

5.5.4. Capacitación VMware vSphere: Operate, Scale and Secure

La capacitación VMware vSphere: Operate, Scale and Secure [V8] está diseñada para brindar conocimiento en la gestión avanzada de VMware vSphere 8. Se enfoca en la configuración, escalabilidad y seguridad de entornos virtualizados, cubriendo desde la administración de redes y almacenamiento hasta la protección y recuperación de máquinas virtuales.

A. Metodología

Esta capacitación tiene un enfoque teórico con ejemplos prácticos. Se utilizarán los siguientes métodos de enseñanza:

- ✓ Presentaciones teóricas: Explicación de conceptos clave y mejores prácticas.
- ✓ Ejemplos prácticos: Guía y muestra en vivo en el ambiente real de VMware vSphere para reforzar el aprendizaje.
- ✓ Espacios de preguntas y respuestas: Interacción para aclarar dudas.
- ✓ Duración: dos (2) días.

B. Incluye:

- ✓ Conceptos clave de VMware vSphere 8.
- ✓ Gestión de seguridad, acceso y monitoreo de entornos virtualizados.
- ✓ Administración de alta disponibilidad y recuperación de máquinas virtuales.
- ✓ Estrategias de escalabilidad y optimización del rendimiento.
- ✓ Escenarios prácticos con resolución de problemas.
- ✓ Certificado de participación provisto por el Consorcio EMDOC.
- ✓ Capacitación para cinco (5) ingenieros de la JCE.
- ✓ La capacitación será impartida en las instalaciones de la JCE.

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

EMDOC

Objetivos de la Capacitación

Al finalizar la capacitación, los participantes podrán:

1. Administrar un VMware Tools Repository.
2. Operar vSphere Replication y recuperar máquinas virtuales replicadas.
3. Gestionar recursos de máquinas virtuales mediante Resource Pools.
4. Administrar redes y almacenamiento para entornos empresariales complejos.
5. Implementar alta disponibilidad en VMware vCenter Server.
6. Monitorear el rendimiento de vCenter, ESXi y máquinas virtuales.

Temario de la Capacitación

1. Introducción al Curso
2. Operaciones con Máquinas Virtuales
   - Administración de VMware Tools Repository.
   - Soluciones de respaldo y restauración de VMs.
   - Visualización de configuración de vSphere Replication y Site Recovery.
3. Gestión de Clústeres en vSphere
   - Visualización y administración de Resource Pools.
   - Funcionamiento de vCLS (vSphere Cluster Services).
4. Administración de vCenter y ESXi
   - Programación de respaldos de vCenter.
   - Visualización de alta disponibilidad en vCenter.
   - Uso de Host Profiles para la gestión de ESXi.
5. Monitoreo en vSphere
   - Factores clave que afectan el rendimiento de VMs.
   - Uso de herramientas de vCenter para análisis de recursos.
6. Seguridad y Control de Acceso
   - Estrategias de seguridad en vCenter, ESXi y VMs.

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

EMDOC
CONSORCIO

5.5.5. Capacitción HPE ProLiant Gen11 Server Management with iLO 6

La capacitación de HPE ProLiant Gen11 Server Management with iLO 6 está diseñado para administradores e ingenieros que necesitan aprender a configurar, actualizar, monitorear y gestionar servidores HPE ProLiant Gen11 utilizando herramientas de administración embebidas como Integrated Lights-Out (iLO) 6.

Esta capacitación cubre desde la configuración inicial del hardware hasta la supervisión avanzada y actualización del firmware, proporcionando un enfoque integral para la gestión eficiente de servidores HPE en entornos empresariales.

Metodología
La capacitación combina teoría con ejemplos prácticos en un entorno real. Se utilizan los siguientes métodos de enseñanza:

- ✓ Presentaciones teóricas: Explicación detallada de conceptos clave.
- ✓ Ejemplos prácticos: Guía y muestra en vivo de servidores y herramientas en tiempo real.
- ✓ Interacción en sesiones de proguntas y respuestas.
- ✓ Duración: un (1) día.

Incluye:

- ✓ Administración de servidores HPE ProLiant Gen11.
- ✓ Gestión de iLO 6 para monitoreo y administración romota.
- ✓ Métodos para actualización de firmware con SPP y SUM.
- ✓ Visualización de configuración de seguridad, rendimiento y energía.
- ✓ Certificado de participación provisto por el Consorcio EMDOC.
- ✓ Capacitación para cinco (5) ingenieros de la JCE.
- ✓ La capacitación será impartida en las instalaciones de la JCE.

5.5.6. Objetivos de la Capacitación

Al finalizar el curso, los participantes serán capaces de:

1. Diferenciar las características de los servidores HPE ProLiant Gen11 y sus opciones de hardware y software.
2. Operar herramientas de administración embebide como iLO 6, UEFI ROM, y Intelligent Provisioning.
3. Visualizar medidas de seguridad y monitoreo para optimizar el rendimiento y consumo energético.
4. Monitorear servidores utilizando la interfaz de iLO 6, comandos REST y herramientas en la nube.
5. Actualizar el firmware de los servidores utilizando Service Pack for ProLiant (SPP) y Smart Update Manager (SUM).
6. Diagnosticar y solucionar problemas utilizando herramientas como Active Health System (AHS) y UEFI Embedded Diagnostics.

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

EMDOC

Temario de la Capacitación

1. Introducción al Hardware de HPE ProLiant Gen11
   - Características de los servidores Gen11.
   - Opciones de hardware y software.
   - Seguridad, garantía y soporte.
2. Introducción a las Herramientas de Administración
   - Gestión embebida en HPE ProLiant.
   - Uso de iLO 6, UEFI ROM, Intelligent Provisioning y Active Health System.
   - Gestión basada en la nube y Baseboard Management Controller (BMC).
3. Administración con iLO 6
   - Acceso remoto y administración de servidores.
   - Configuración de seguridad y políticas de acceso.
   - Opciones de gestión de energía y temperatura.
4. Actualización del Servidor
   - Métodos de actualización de firmware.
   - Uso de Service Pack for ProLiant (SPP) y Smart Update Manager (SUM).
   - Procedimientos de actualización de iLO 6.
5. Monitoreo del Servidor
   - Uso de iLO 6 y herramientas de monitoreo.
   - Configuración de alertas y análisis de rendimiento.
   - Verificación de firmware y monitoreo con RESTful API.
6. Diagnóstico y Solución de Problemas
   - Herramientas de diagnóstico embebidas en UEFI e iLO.
   - Descarga y análisis de logs con Active Health System (AHS).
   - Indicadores LED y su interpretación.
7. Recursos y Soporte
   - Uso del HPE Support Center y My Software Center Dashboard.
   - Acceso a actualizaciones y materiales de soporte.
   - Pasos siguientes para continuar el aprendizaje.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

6. Premisas y Entregables

- ✓ El Consorcio EMDOC se hace responsable de la entrega de todos los servicios de instalación y configuración de los equipos ofertados.
- ✓ El Consorcio EMDOC se hace responsable de la realización de las configuraciones, actualizaciones y mejoras de software necesarias para la integración de los nuevos equipos.
- ✓ Nuestra propuesta incluye todo el hardware, software y licenciamientos necesarios para la instalación y operación tal y como es requerido.
- ✓ Nuestra propuesta incluye soporte de tipo proactivo con SLA de atención 24x7x4 con una duración de cinco (5) años a partir de la fecha de aceptación por escrito por parte de la Junta Central Electoral y puesta en marcha de los equipos.
- ✓ Nuestra propuesta incluye equipos nuevos no reconstruidos.
- ✓ Nuestra propuesta incluye plan de trabajo detallado en la propuesta técnica en el cual se especifica de forma clara todos los pasos a ejecutar durante el proceso de implementación de los equipos ofertados.
- ✓ Nuestra propuesta incluye proveer, instalar y configurar todos los equipos, hardware y licencias con las características técnicas mencionadas según la tabla de referencias. La solución propuesta está integrada y certificada de fábrica en todos sus componentes como un solo producto según cada lote.
- ✓ Nuestra propuesta incluye la entrega de todos los equipos en completa operación, a satisfacción de la entidad, con todos los componentes solicitados incluidos.
- ✓ Se incluyen todas las hojas técnicas (DataSheets) de los propuestos ofertados. así como el link correspondiente del fabricante.
- ✓ Nuestra propuesta incluye equipos nuevos de fábrica, no se incluyen equipos reemplazos o remanufacturados.
- ✓ Se incluyen cartas del fabricante en la cual el Consorcio EMDOC a través de los miembros del consorcio cuenta con las debidas autorizaciones a ofrecer los bienes y servicios presentados en nuestra oferta.
- ✓ Se incluye carta del fabricante en la cual se indica que todos los equipos ofertados son nuevos, no usados, no remanufacturados, ni reparados y que los mismos no se encuentran descontinuados ni anunciados fuera de vida.
- ✓ Nuestra propuesta incluye la asignación de un gerente de proyectos certificado PMP dedicado 100% de su tiempo a la implantación de todas las soluciones ofertadas en este lote durante todo el tiempo que sea necesario y requerido por la institución hasta la conclusión y recepción del proyecto. Este Gerente de proyecto es empleado fijo de uno de los miembros del Consorcio EMDOC con más de 6 meses en la empresa.

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

EMDOC
CONSORCIO

R59-1

Datasheets

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

VERIDOS

IDENTITY SOLUTIONS

by Giesecke+Devrient
and Bundesdruckerei

260

[redacted]KI

[redacted]-0001

CONSORCIO EMDOC

EMDOC
CONSORCIO

Santo Domingo, R.D.

VERIDOS

IDENTITY SOLUTIONS

by Giesecke+Devrient and Bundesdruckerei

261

CONTENIDO

1 Sistema PKI 3

1.1 Visión general del sistema PK 3

1.2 Requisitos del sistema 4

1.3 Integración del sistema 4

1.3.1 Autenticación pasiva PKI 4

1.3.2 Sistema PKI de control de acceso ampliado 5

1.3.3 Firma digital PKI 6

1.3.4 ISO 18013-5 PKI 7

1.4 Interfaces del sistema 8

1.4.1 Autoridad de certificación con firma de país (CSCA 8

1.4.2 Autoridad de certificación verificadora de países (CVCA) 8

1.4.3 Firma digital PKI 9

1.4.4 Autoridad emisora Autoridad de certificación (IACA) 9

1.5 Funcionalidad 10

1.5.1 Autoridad de certificación con firma de país (CSCA 10

1.5.2 Autoridad de certificación de verificación de país (CVCA) 10

1.5.3 Firma digital PK 11

1.5.4 Autoridad emisora Autoridad de certificación (IACA) 12

1.5.5 Requisitos no funcionales 13

1.6 Referencias 14

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

VERIDOS

IDENTITY SOLUTIONS

by Giesecke+Devrient and Bundesdruckerei

262

1 Sistema PKI

1.1 Visión general del sistema PKI

En esta sección se describen los componentes de la PKI necesarios para los sistemas de documentos de identidad electrónico y de la tarjeta de identificación digital:

- Tarjeta e D
  - Autenticación pasiva (PA) PKI
  - Control de acceso ampliado (EAC) PKI
  - PKI para digital
- Identificación móvil
  - ISO 18013-5 PKI

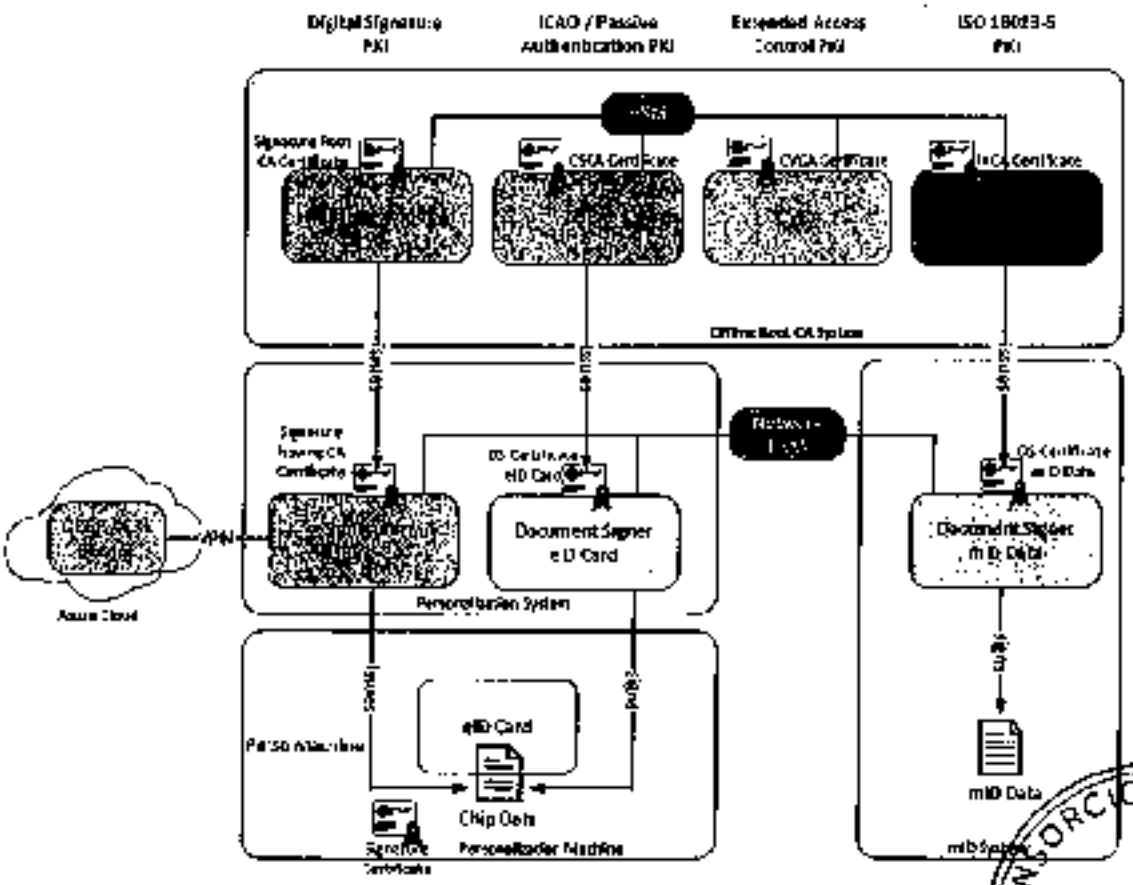


Figura 1 : Visión general de la infraestructura PKI

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo

1.2 Requisitos del sistema

El sistema propuesto soportará la personalización de documentos de identidad electrónicos y datos de identificación móviles aplicando los siguientes métodos de seguridad relacionados con la PKI:

- Autenticación pasiva (PA)
- Control de acceso ampliado (CAE)
- Certificados para firmas digitales
- ISO 18013-5 PKI

La autenticación pasiva (PA) garantiza la autenticidad e integridad de los datos del documento de identidad electrónico almacenados en el chip. Garantiza que los datos del chip proceden de la autoridad emisora legítima y que los datos no han sido manipulados. La PKI para la autenticación pasiva (PA) debe cumplir las especificaciones de la OACI descritas en el Doc 9303-12 y también se conoce como PK. de la OACI. Los objetos de la PKI de PA (certificados, CRL, listas maestras) deben intercambiarse con otros Estados y cargarse en sus puestos de control fronterizo. Todos los certificados emitidos y gestionados de este sistema cumplen la norma X.509v3.

El control de acceso ampliado (EAC) garantiza la autenticidad y confidencialidad de los datos biométricos almacenados en el chip. Garantiza que los datos biométricos sólo puedan ser leídos por un lector autorizado y que el chip sea auténtico. La PKI para el control de acceso ampliado debe cumplir la directriz técnica TR-03110 de la BSI
Ambos sistemas deben proporcionar interfaces normalizadas para interactuar con el sistema de personalización de tarjetas de identidad electrónica y otros sistemas.

Los certificados de **firma digital** permiten crear firmas digitales de confianza con la tarjeta eID. El material clave para el certificado de firma se generará durante la personalización de la tarjeta y se solicitará a la PKI central un certificado conforme a la norma X.509v3 que se escribirá en la tarjeta.

ISO 18013-5 PKI garantiza la autenticidad y la integridad de las identidades móviles y de los datos de los permisos de conducir móviles (mDL). Garantiza que los datos proceden de la autoridad emisora legítima y que no han sido manipulados. La PKI debe cumplir la norma ISO/IEC 18013-5:2021(en) - Personal identification - ISO-compliant driving licence - Part 5: Mobile driving licence (mDL) application.

1.3 Integración del sistema

1.3.1 Autenticación pasiva PKI

La autenticación pasiva se utiliza para garantizar la autenticidad de los datos del chip, que están estructurados en una estructura lógica de datos (LDS). Para la autenticación pasiva se necesita una autoridad de certi

CONSORCIO EMDOC

de firma de país (CSCA) y un firmante de documentos (DS). La siguiente imagen muestra la vista lógica de los componentes necesarios.

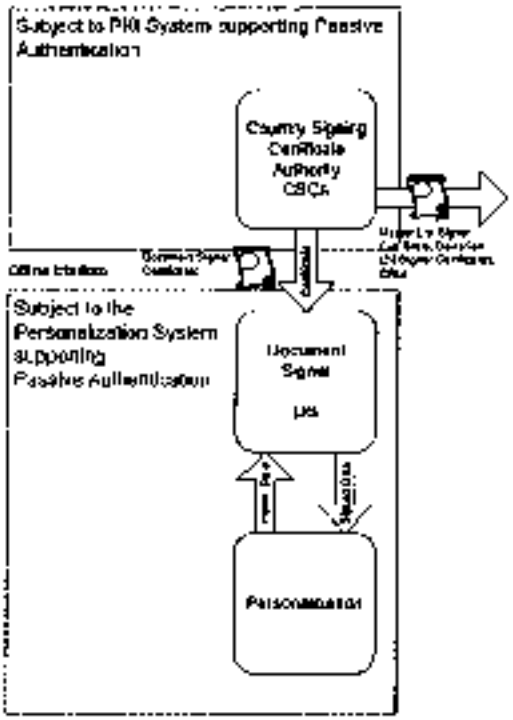


Figura2 : Infraestructura PKI para autenticación pasiva

1.3.2 Sistema PKI de control de acceso ampliado .

El control de acceso ampliado (EAC) protege los datos biométricos almacenados en el chip frente a accesos no autorizados

Las huellas dactilares se protegen mediante el protocolo EAC, tal como se especifica en BSI TR-03110 v1.11. EAC es un mecanismo de autenticación mutua basado en PKI asimétrica. Se utilizan certificados especiales verificables mediante tarjeta para definir los derechos de los terminales utilizados para la verificación de documentos.

Este sistema PKI comprende únicamente la CVCA. Al crear las claves y el certificado CVCA y escribir este anclaje de confianza en el chip, el sistema de tarjeta de identidad electrónica está preparado para la ampliación mediante datos biométricos de huellas dactilares.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo

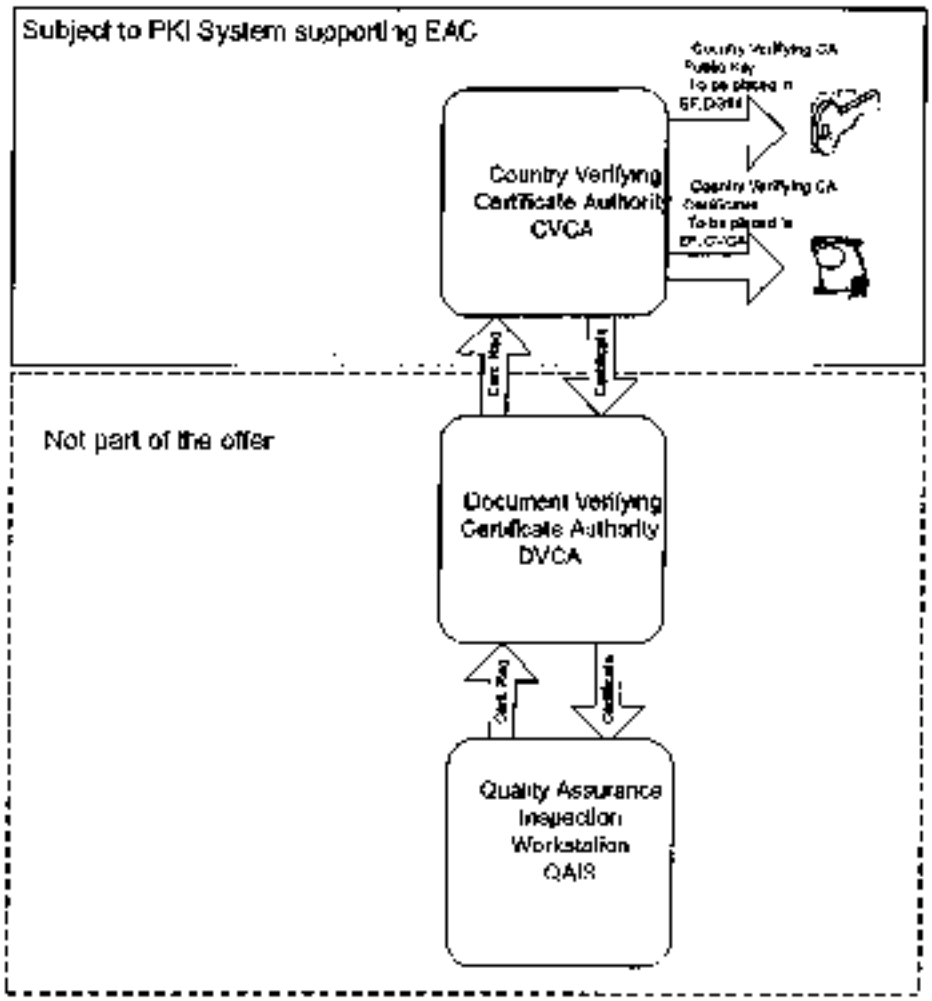


Figura3 : Infraestructura EAC para sistemas de personalización

1.3.3 Firma digital PKI

La PKI de firma digital se encarga de emitir certificados de firma para cada tarjeta eID personalizada. Los certificados están personalizados para el titular de la tarjeta. Éste puede utilizar el certificado y la clave de firma para crear firmas digitales hables localmente en el ordenador personal o en otros dispositivos que admitan la integración del documento de identidad electrónico. La PKI consta de dos niveles: la CA raíz, que [illegible]

EMDOC CONSORCIO Santo Domingo

de línea, y la CA emisora, con conexión en línea al sistema de personalización del documento de identidad electrónico

El estado de cada certificado emitido es gestionado por el sistema CA y replicado a Certificate Status Server. A intervalos regulares se crean CRL que contienen los números de serie de todos los certificados revocados. También estas CRL se replican a este servidor. El servidor de estado de certificados publica la información a través del protocolo OCSP (Online Certificate Status Protocol) y mediante la descarga de CRL. El Servidor de Estado de Certificados está alojado en un sistema en la nube proporcionado por el Cliente.

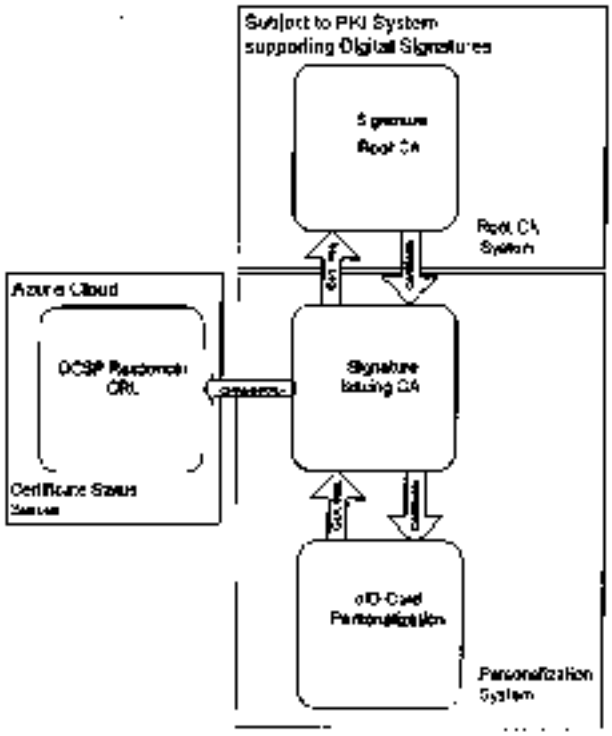


Figura 1 : PKI de Firma para sistemas de personalización

1.3.4 ISO 18013-5 PKI

La PKI ISO es muy similar a la PKI de autenticación pasiva. Se utiliza para garantizar la autenticidad de los datos de Identidad móviles. Consta de una Autoridad Emisora Autoridad de Certificación (IACA) y un Firmante de Documentos (DS). La siguiente imagen muestra la vista lógica de los componentes necesarios.

CONSORCIO EMDOC
EMDOC
CONSORCIO

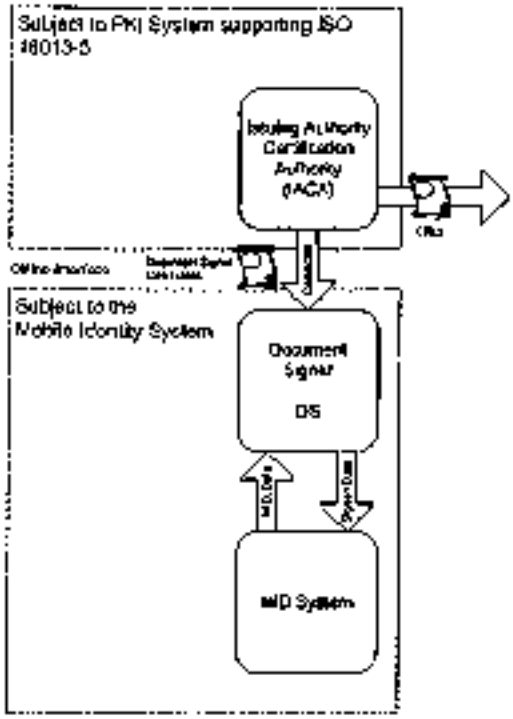


Figura5 : Infraestructura PKI para ISO PKI

1.4 Interfaces del sistema

1.4.1 Autoridad de certificación con firma de país (CSCA

El CSCA funciona sin conexión. Todas las interfaces con otros sistemas se basan en archivos:

- Archivos de solicitud de certificado en formato PKCS#10
- Archivos de certificado según X509v3 en formato binario DER o ASCII PEM
- Archivos de listas de revocación de certificados (CRL) según X509v3 en formato DER binario

1.4.2 Autoridad de certificación verificadora de países (CVCA)

El CSCA funciona sin conexión. Todas las interfaces con otros sistemas se basan en archivos:

- Archivos de solicitud de certificado en formato PKCS#10

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo

- Ficheros de certificados según la norma ISO 7810 8 (Certificados verificables mediante tarjets)

1.4.3 Firma digital PKI

1.4.3.1 Firma CA raíz

La CA Raiz de firma funciona sin conexión. Todas las interfaces con otros sistemas se basan en archivos:

- Archivos de solicitud de certificado en formato PKCS#10
- Archivos de certificado según X509v3 en formato binario DER o ASCII PEM
- Archivos de listas de revocación de certificados (CRL) según X509v3 en formato DER binario

1.4.3.2 Firma CA emisora

La CA emisora de firmas funciona en línea. Las interfaces con otros sistemas se basan en la web (REST API).

- Solicitud de certificados
- Ficheros de certificados
- Lista de revocación de certificados (CRL) según X509v3
- Información sobre el estado del certificado

1.4.3.3 Servidor de estado de certificados

El servidor de estado de certificados funciona en un servicio en la nube. Proporciona una interfaz de importación a la CA emisora para obtener información de estado y CRL y publica la información en Internet.

- Importación de información sobre el estado de los certificados
- Respuestas OCSP a través de http
- Descarga de CRL a través de http

1.4.4 Autoridad emisora Autoridad de certificación (IACA)

La IACA funciona sin conexión. Todas las interfaces con otros sistemas se basan en archivos:

- Archivos de solicitud de certificado en formato PKCS#10
- Archivos de certificado según X509v3 en formato binario DER o ASCII PEM
- Archivos de listas de revocación de certificados (CRL) según X509v3 en formato DER binario

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

1.5 Funcionalidad

1.5.1 Autoridad de certificación con firma de país (CSCA

De acuerdo con el Informe Técnico de la OACI Doc9303 Parte 12 "Infraestructura de Clave Pública para MRTDs", esta PKI consiste en una Autoridad de Certificación de Firma de País (CSCA) como CA Raíz. La principal tarea de la CSCA es la emisión de los certificados de firmante de documentos

El CSCA utiliza un módulo de seguridad de hardware (HSM) para la generación segura de claves, la protección de claves de hardware y la gestión del ciclo de vida de las claves, y es capaz de realizar operaciones criptográficas asimétricas con longitudes y tipos de clave conformes con la OACI.

El CSCA ofrece las siguientes funciones:

- Generación y renovación de una clave de firma de país.
- Generación, emisión y renovación de certificados CSCA y CSCA link autofirmados
- Generación y emisión de certificados de firmante de documentos (X.509v3) solicitados mediante PKCS#10.
- Generación y emisión de certificados de firmante de lista maestra (X.509v3) solicitados mediante PKCS#10.
- Generación y emisión de certificados de firmante de lista de desviación (X.509v3) y solicitados mediante PKCS#10.
- Generación y exportación de listas de revocación de certificados
- Protección de claves por hardware.
- Destrucción de las claves generadas de forma segura (tras su caducidad)

1.5.2 Autoridad de certificación de verificación de país (CVCA) .

La Autoridad de Certificación verificadora del país es el nivel raíz de la PKI de la CAO.

La CVCA ofrece las siguientes funciones:

- Generación y renovación de una clave de verificación de país.
- Generación, emisión y renovación de certificados CVCA autofirmados y certificados CVCA de enlace
- Firma de certificados de verificador de documentos para un verificador de documentos
- Exportación de los certificados
- Protección de claves de hardware

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

- Destrucción de las claves generadas de forma segura (tras su caducidad)

1.5.3 Firma digital PKI

1.5.3.1 Firma CA raíz

La CA Raíz de Firma es el nivel raíz de la PKI de Firma Digital. Sirve como ancla de confianza para esta PKI.

La CA Raíz de Firma proporciona la siguiente funcionalidad.

- Generación y renovación de una clave de CA raíz
- Generación y emisión de certificados de CA emisora
- Generación y emisión de CRL
- Protección de claves por hardware.
- Destrucción de las claves generadas de forma segura (tras su caducidad).

1.5.3.2 Firma CA emisora

La CA emisora de firmas proporciona la siguiente funcionalidad.

- Generación y renovación de una clave de CA emisora
- Generación y emisión de solicitudes de certificados de CA emisora
- Importación de certificados de CA emisoras
- Generación y emisión de CRL
- Publicación de información sobre el estado de los certificados
- Verificación de la identidad y autorización de los solicitantes de certificados
- Generación de certificados de firma solicitados por el sistema de personalización
- Protección de claves por hardware.
- Destrucción de las claves generadas de forma segura (tras su caducidad)

1.5.3.3 Servidor de estado de certificados

El servidor de estado de certificados ofrece las siguientes funciones:

- Importación y almacenamiento de información sobre el estado de los certificados y CRL
- Respuesta a las solicitudes de la OSCP

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

- Respuesta a las solicitudes de descarga de CRL

La CA Emisora de Firma es responsable de la producción de certificados de firma durante la personalización de las tarjetas eID. Está alojada en una máquina virtual (VM) dedicada en el hipervisor de la red interna. Para la gestión y protección de las claves privadas de la CA emisora se utilizan HSM de red. Estos HSM se compartirán con el sistema de personalización mID, pero las claves de las CA emisoras se gestionarán en una sección (ranura) dedicada de los HSM.

Según se requiera, la CA raíz y la CA emisora utilizarán la especificación de clave RSA con un tamaño de clave de 4096 bits, los certificados de usuario (ciudadano) se emitirán con un tamaño de clave de 2048 bits. Todos los certificados se basan en las normas X.509v3 y RFC 5280. A petición también se pueden utilizar curvas elípticas según las especificaciones NIST y Brainpool.

1.5.4 Autoridad emisora Autoridad de certificación (IACA)

De conformidad con la norma ISO/IEC 18013-5:2021(en) - Personal identification - ISO-compliant driving licence - Part 5: Mobile driving licence (mDL) application, esta PKI consta de una Autoridad de Certificación Emisora (IACA) como CA Raíz. La tarea principal de la IACA es la emisión de los certificados Document Signer para las identidades digitales móviles

La IACA utiliza un módulo de seguridad de hardware (HSM) para la generación segura de claves, la protección de claves de hardware y la gestión del ciclo de vida de las claves, y es capaz de realizar operaciones criptográficas asimétricas con longitudes y tipos de clave conformes a ISO. La principal diferencia con el CSCA según la OACI es el formato de clave utilizado en el certificado raíz.

La IACA ofrece las siguientes funciones:

- Generación y renovación de una clave de firma de país.
- Generación, emisión y renovación de certificados autofirmados IACA e IACA link
- Generación y emisión de certificados de firmante de documentos (X.509v3) solicitados mediante PKCS#10.
- Generación y exportación de listas de revocación de certificados
- Protección de claves por hardware.
- Destrucción de las claves generadas de forma segura (tras su caducidad).

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo RD

1.5.5 Requisitos no funcionales

1.5.5.1 Disponibilidad del sistema

Todos los sistemas Root PKI, la CSCA, la CVCA, la IACA y la CA Raiz de Firma, están alojados en un sistema de servidor por HSM integrado. Después de cada operación se realiza una copia de seguridad del sistema (incluido el material de claves del HSM).

Un dispositivo de servidor redundante con HSM se mantiene en una ubicación separada. En caso de fallo del hardware primario, la copia de seguridad se restaurará en el hardware de reserva. Este sistema de copia de seguridad proporcionará una funcionalidad idéntica a la del sistema primario y garantizará la continuación sin problemas de todas las operaciones.

1.5.5.2 Seguridad del sistema

Todos los sistemas de la PKI raiz, la CSCA, la CVCA, la IACA y la CA raiz de firma, están alojados en un sistema de servidor aislado que funciona en un entorno de alta seguridad. Sólo se accede al sistema si es necesario realizar una operación.

El sistema admite la autenticación de dos factores con token y PIN para que los operadores inicien sesión.

Todas las conexiones de red están protegidas por cifrado mediante conexiones TLS autenticadas mutuamente.

La copia de seguridad del material clave está protegida por un conjunto de tarjetas inteligentes con PIN individuales. La restauración del material de claves requiere la presencia de un número mínimo definido de tarjetas inteligentes.

1.5.5.3 Despliegue del sistema

El Sistema PKI se desplegará en el Centro de Datos de la sede central, excepto el Servidor de Estado de Certificados de la PKI de Firma Digital que se alojará en un servicio en la nube.

Los módulos de seguridad de hardware (HSM) certificados según se utilizan para almacenar y gestionar de forma segura claves criptográficas y ejecutar funciones criptográficas en un entorno reforzado. El HSM de red se despliega en una disposición redundante con un segundo dispositivo conectado a la red. Los dispositivos HSM ofrecidos están certificacos conforme a Common Criteria (CC) EAL4+ para sus basados en el perfil de protección eIDAS EN 419 221-5 [4].

Se utiliza un sistema de servidor dedicado con PCI HSM integrado para alojar la CSCA fuera de línea, la CVCA, la IACA y la CA raíz de firma.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

Se desplegará un sistema de prueba para los distintos sistemas PKI en un entorno independiente.

1.6 Referencias

[1] Doc. 9303 de la OACI, Documentos de viaje legibles por máquina, octava edición 202, Parte 12: Infraestructura de clave pública para MRTD.

[2] BSI TR-03110, Mecanismos avanzados de seguridad para documentos de viaje legibles por máquina

[3] ISO/IEC 18013-5:2021(en) - Personal identification - ISO-compliant driving licence - Part 5: Mobile driving licence (mDL) application (Identificación personal - Permiso de conducción conforme a ISO - Parte 5: Aplicación de permiso de conducción móvil)

[4] CSN EN 419221-5, Perfiles de protección para módulos criptográficos TSP - Parte 5: Módulo criptográfico para servicios de confianza.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo

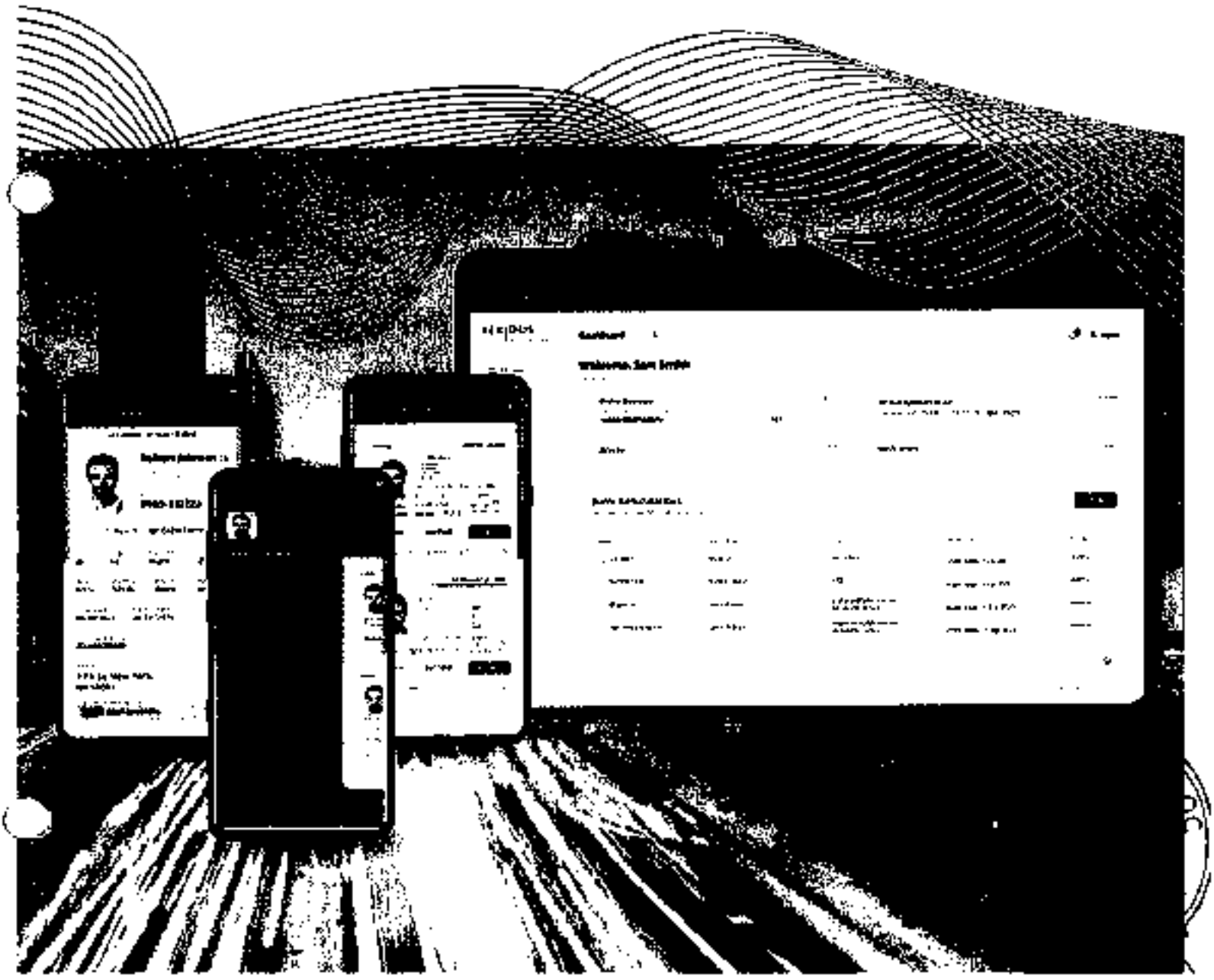
VERIDOS

IDENTITY SOLUTIONS

FECHA:February 25

274

VeriGO MobileID Descripción General de la Plataforma



CONTENIDO

1 Introducción a la guía completa 6

1.1 Visión general y orientación 6

La honorable comisión de la JCE pretende modernizar y mejorar los servicios al ciudadano en consonancia con las directivas vigentes mediante la integración de tecnologías avanzadas de seguridad para mejorar la autenticidad y protección de los documentos de identidad. La iniciativa refuerza los servicios del Registro Civil y del Documento de Identidad al tiempo que mitiga los riesgos de fraude y falsificación 6

1.2. Glosario 6

2 Resumen de la plataforma VeriGO MobileID 8

2.1. Contenido de esta sección 8

2.2. Visión general de la plataforma VeriGO MobileID 8

2.3. Usuarios de la plataforma VeriGO MobileID 9

2.4. Verificación de documentos de identidad con la plataforma VeriGO MobileID 9

2.5. Cumplimiento de las normas internacionales 9

2.6. Lanzamiento e implantación de la plataforma VeriGO MobileID 9

2.7. Digitalización y combinación de documentos de alta seguridad 10

2.8. Rendimiento de la plataforma VeriGO MobileID 11

2.8.1. Rapidez y capacidad de respuesta 11

2.8.2. Fiabilidad 11

2.8.3. Precisión 11

2.8.4. Experiencia del usuario 11

2.9. Escalabilidad de la plataforma VeriGO MobileID 11

2.9.1. Aumento de la carga 11

2.9.2. Infraestructura flexible 12

2.9.3. A prueba de futuro 12

3 Características de la plataforma VeriGO MobileID 13

3.1. Contenido de esta sección 13

3.2. Introducción a las características de la plataforma VeriGO MobileID 13

3.3. Características principales 13

3.3.1. Múltiples identidades con credenciales multifactor 13

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo

3.3.2. Verificación y autenticación sólidas de la identidad 14
3.3.3. Consentimiento del usuario 14
3.3.4. Propiedad de la identidad 14
3.3.5. Inyección del verificador 14
3.3.6. Gobernanza de la privacidad de los datos 14
3.4. Funciones auxiliares de la plataforma VeriGO MobileID 14
3.4.1. Notificaciones push 14
3.4.2. Gestión de perfiles 15
3.5. Programa de mantenimiento 16
3.5.1. Actualizaciones y parches periódicos del software 16
3.5.2. Supervisión continua de la seguridad 16
3.5.3. Planes de copia de seguridad y recuperación de datos 16
3.5.4. Supervisión y optimización del rendimiento 16
3.5.5. Asistencia y formación de usuarios 16
4 La tecnología de la plataforma VeriGO MobileID 17
4.1. Contenido de esta sección 17
4.2. Introducción a la tecnología de la plataforma VeriGO MobileID 17
4.3. La tecnología fundamental de la plataforma VeriGO MobileID 17
4.4. Tecnología en la que pueden confiar los verificadores 18
4.5. Orgullosos de estar a la vanguardia de los avances tecnológicos 19
4.6. Tecnologías utilizadas en la plataforma VeriGO MobileID 19
5 La seguridad de la plataforma VeriGO MobileID 20
5.1. Contenido de esta sección 20
5.2. Introducción a los sistemas de seguridad de la plataforma VeriGO MobileID 20
5.3. Mantenimiento de seguridad 20
5.4. Directrices de seguridad de la plataforma VeriGO MobileID 21
5.5. Normas de seguridad de la plataforma VeriGO MobileID 21
5.6. Cifrado de extremo a extremo 22
5.7. Seguridad del usuario en la plataforma VeriGO MobileID 22
5.7.1. Funciones criptológicas 22
5.7.2. Procesos de inscripción sólidos 23

CONSORCIO EMDOC
EMDOC
Santo Domingo

5.8. Aprovisionamiento: procesos de inscripción seguros 23
5.9. Tres ejemplos de procesos de inscripción seguros 24
5.9.1. Ejemplo uno | seguridad de los usuarios: inscripción en persona 24
5.9.2. Ejemplo dos | seguridad de los usuarios: inscripción en línea 25
5.9.3. Ejemplo tres | seguridad de los usuarios: autoinscripción totalmente automatizada 25
5.10 Seguridad del verificador en la plataforma VeriGO MobileID 26
5.11. Proteja los documentos de identidad de accesos no autorizados 27
5.12. Protección contra la falsificación 28
5.13. Cumplimiento de las normas 28
5.13.1. Cumplimiento de las normas internacionales 29
5.13.2. Tipos y formatos de credenciales verificables 29
5.13.3. Datos de identificación de la persona (PID) 30
5.13.4. Atestación electrónica cualificada de atributos (QEAA) 30
5.13.5 Atestación electrónica de atributos (AEA) 30
5.13.6. Formatos de credenciales verificables 31
6 Integración de la plataforma VeriGO MobileID 32
6.1. Contenido de esta sección 32
6.2. Introducción a la integración de la plataforma VeriGO MobileID 32
6.3. Tipos de capacidades de integración 33
6.3.1. Integración de datos 33
6.3.2 Integración de procesos 33
6.3.3. Integración de aplicaciones 33
6.3.4 Integración API 33
6.3.5. Integración de microservicios 33
6.4. Tecnologías de integración 33
6.4.1. Plataforma de integración como servicio (iPaaS 33
6.4.2. Plataforma de gestión de API 33
6.4.3. Arquitectura de microservicios 33
6.5. Componentes clave de integración de la plataforma VeriGO MobileID 34
6.5.1. Biometría 34
6.5.2. Pruebas de conocimiento-cero 34

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

6.5.3. Imágenes Dockerizadas 34
6.5.4. Herramientas de control 34
6.6. Planificación de la integración de la plataforma VeriGO MobileID 34
6.7. Diseño de la integración de la plataforma VeriGO MobileID 35
6.8. Desarrollo de la integración de la plataforma VeriGO MobileID 35
6.9. Pruebas de integración de la plataforma VeriGO MobileID 35
6.10. Diversidad en los datos de formación 36
7 Casos prácticos Usuarios de la plataforma VeriGO MobileID 37
7.1. Contenido de esta sección 37
7.2. Caso práctico 1 37
7.3. Caso práctico 2 38
7.4. Casos de usuarios adicionales 38
8 Preparar para el futuro la plataforma VeriGO MobileID 39
8.1. Contenido de esta sección 39
8.2. Oportunidades ilimitadas 39
8.3. Herramienta de comunicación 39
8.4. Herramienta de administración 39

CONSORCIO EMDOC CONSORCIO Santo Domingo

1 Introducción a la guía completa

1.1. Visión general y orientación

La honorable comisión de la JCE pretende modernizar y mejorar los servicios al ciudadano en consonancia con las directivas vigentes mediante la integración de tecnologías avanzadas de seguridad para mejorar la autenticidad y protección de los documentos de identidad. La iniciativa refuerza los servicios del Registro Civil y del Documento de Identidad al tiempo que mitiga los riesgos de fraude y falsificación.

Este documento ofrece una visión global de la Plataforma VeriGO MobileID en las secciones 2 a 8. Contiene información detallada sobre cada elemento de la Plataforma VeriGO MobileID. Además, los capítulos 9 a 12 ofrecen una explicación técnica detallada de cómo la Plataforma VeriGO MobileID cumple plenamente los requisitos del PUNTO IV - ESPECIFICACIONES TÉCNICAS TARJETA DE IDENTIDAD DIGITAL de la licitación de Servicios de Identidad Digital mID correspondiente para la JUNTA ELECTORAL CENTRAL DE LA REPÚBLICA DOMINICANA, Referencia de licitación: JCE-CL-LPI-2024-01.

1.2. Glosario

El glosario existe para definir el lenguaje técnico e industrial.

Glosario	
El cliente	La organización que lanzará VeriGO MobileID
Organismo emisor	La administración general que expide el documento de identidad auténtico
Usuario	El usuario individual, o ciudadano, que utiliza la aplicación VeriGO MobileID
Verificadores	Los trabajadores oficiales que comprueban los documentos de identidad para confirmar la identidad de un usuario, es decir, agentes de policía, banqueros, agentes inmobiliarios. Con VeriGO MobileID, los verificadores pueden confirmar la identidad digitalmente
Plataforma Vericore EIS	La plataforma Veridos de inscripción de usuarios y expedición de credenciales
mDl	Permiso de conducir movil. El VeriGO MobileID puede almacenar documentos de identidad como permisos de conducir
OTP	Contraseña de un solo uso. Un pin seguro temporal válido para una sola sesión.

CONSORCIO EMDOC CONSORCIO Santo Domingo

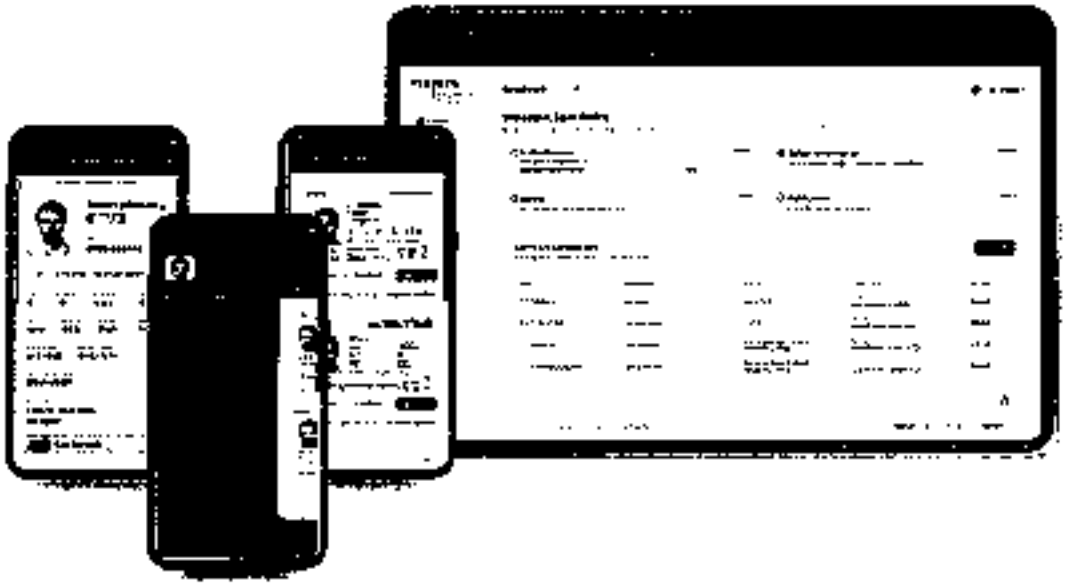
PKI	Infraestructura de clave pública
SCRUM	SCRUM es un marco de colaboración ágil para el desarrollo de software
BLE	Bluetooth de baja energía
OIDC4VP	OpenID connect para presentaciones verificables
REST	Transferencia del estado de representación
fido2	Fast Identity Online: alianza para la normalización de la autenticación en línea
Criptografía	La criptografía utiliza algoritmos codificados para proteger y ocultar la información transmitida, de modo que sólo pueda ser leída por quienes tienen permiso para ello.
Docker	Un contenedor es una unidad estándar de software que empaqueta el código y todas sus dependencias para que la aplicación se ejecute de forma rápida y fiable de un entorno informático a otro
OpenID connect (OAuth 2.0)	Autenticación abierta
SAML 2.0	Lenguaje de marcado de aserción de seguridad. Norma abierta basada en XML para el intercambio de datos de autenticación y autorización.
RLS	Separación por filas
PII	información personal identificable
OIDC	Open ID Connect: estándar de autenticación
LDAP-AD	Protocolo ligero de acceso a directorios
SCIM 2.0	System for Cross-Domain Identity Management (SCIM) es un protocolo de norma abierta utilizado para simplificar la gestión de identidades y accesos en la nube.
ISO/IEC 18013-5	norma internacional que define las especificaciones de los permisos de conducir móviles (mDL) y su intercambio de datos con el dispositivo electrónico
ISO/IEC 18013-6	prescribe los requisitos para la comprobación de la conformidad del modelo de datos, el compromiso del dispositivo, la transferencia de datos y los mecanismos de seguridad en una aplicación móvil de conducción con la los requisitos de la norma :ISO/IEC 18013-5.
W3C	El Consorcio World Wide Web
AAMVA mDL	Asociación Americana de Administradores de Vehículos de Motor
LDAP-AD	Protocolo ligero de acceso a directorios
AWS-Nube	Amazon Web Service, o AWS, es una plataforma en línea que ofrece soluciones rentables y escalables de computación en nube.
En las instalaciones	La ubicación física del centro de datos
UX	Definición de experiencia de usuario
GDPR	Reglamento general de protección de datos

CONSORCIO EMDOC
EMDOC
CONSORCIO

2 Resumen de la plataforma VeriGO MobileID

2.1.Contenido de esta sección

Esta sección resume la Plataforma VeriGO MobileID sin entrar en detalles técnicos o minuciosos. Esta información es útil para introducir los conceptos de la Plataforma VeriGO MobileID y explicar brevemente su funcionalidad. En secciones posteriores se ofrece información más detallada y específica.



2.2.Visión general de la plataforma VeriGO MobileID

La plataforma VeriGO MobileID es una solución digital para autenticar de forma segura y rápida la identidad de un usuario.

La aplicación para smartphone contiene documentos de identificación aprobados, como permisos de conducir, tarjetas nacionales de identificación y tarjetas sanitarias. VeriGO Mobilities no sustituye a las copias físicas tradicionales de los documentos de identidad, sino que las complementa.

La plataforma VeriGO MobileID permite a los usuarios gestionar documentos de identificación en su smartphone, tanto en línea como fuera de línea.

La plataforma VeriGO MobileID es "sólo móvil". Esto significa que los usuarios no necesitan más dispositivo que un smartphone o una tableta para acceder a la aplicación y a sus documentos de identidad.

CONSORCIO EMDOC

2.3. Usuarios de la plataforma VeriGO MobileID

La plataforma VeriGO MobileID ha sido diseñada para ser lo más intuitiva y sencilla posible. Maximiza la facilidad de uso, manteniendo al mismo tiempo el máximo nivel de seguridad y privacidad.

La accesibilidad es crucial para Veridos. La plataforma VeriGO MobileID se ha desarrollado siguiendo las directrices de accesibilidad al contenido web (WCAG).

La plataforma VeriGO MobileID es apta para usuarios de todo el mundo, siempre que sean mayores de 18 años y dispongan de documentos de identidad aprobados por el organismo emisor.

2.4. Verificación de documentos de identidad con la plataforma VeriGO MobileID

Los verificadores, como los agentes de policía, dependen actualmente de comprobar la identificación de un usuario con un documento físico. Con VeriGO MobileID, los verificadores pueden confirmar la identidad de un usuario a través de su smartphone.

Para lanzar, ejecutar y mantener VeriGO MobileID, Veridos utiliza métodos rigurosos y exhaustivos para verificar los documentos de identificación de un usuario. Los verificadores pueden estar seguros de que los documentos son auténticos y válidos.

2.5. Cumplimiento de las normas internacionales

La plataforma VeriGO MobileID estará en consonancia con las normas internacionales pertinentes, entre las que se incluyen:

- ISO/IEC 18013-5 e ISO/IEC 18013-6 sobre permisos de conducción móviles
- Directrices de implantación de mDL de AAMVA
- Norma del W3C sobre credenciales verificables

Entre estas normas, el conjunto aprobado por la ISO en septiembre de 2021 es actualmente el más maduro y el más completo. Abarca muchos aspectos de las soluciones de documentos de identificación, como el formato de los datos, el cifrado de datos y las tecnologías de transferencia de datos.

2.6. Lanzamiento e implantación de la plataforma VeriGO MobileID

Veridos, en colaboración con El Cliente, lanzará la plataforma VeriGO MobileID por fases. Mediante una selección estratégica de los grupos demográficos de usuarios, la plataforma se irá desplegando gradualmente hasta llegar a toda la población.

CONSORCIO EMDOC
EMDOC
CONSORCIO

Veridos colaborará estrechamente con todas las partes interesadas en las fases de investigación, desarrollo, pruebas y lanzamiento del proyecto.

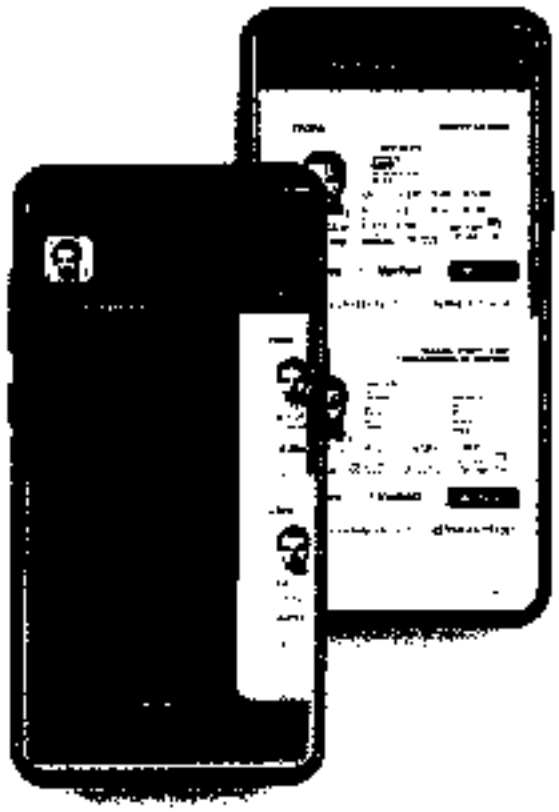
Existen numerosas personalizaciones de la aplicación que Veridos puede implementar de acuerdo con las peticiones del cliente y/o las estipulaciones del organismo emisor. Esto incluye la adaptación de la estética de la aplicación a las plataformas digitales existentes del cliente. Se pueden realizar personalizaciones a medida, así como personalizaciones estándar de la pantalla de inicio de la aplicación y de la paleta de colores.

2.7. Digitalización y combinación de documentos de alta seguridad

Una amplia gama de documentos, como tarjetas de fidelidad, tarjetas de embarque, entradas para eventos y carnés de socio, ya existen en formato digital en los teléfonos inteligentes.

Es un desarrollo natural ampliar estos documentos a documentos formales de identificación. La plataforma VeriGO MobileID permite combinar varios documentos en una sola aplicación, convirtiendo así la app del usuario en un auténtico monedero digital.

Basándose en un exhaustivo y costoso proceso de investigación y desarrollo, Veridos ha desarrollado la plataforma VeriGO MobileID para cumplir las rigurosas normas de seguridad requeridas para la desmaterialización de documentos de alta seguridad.



CONSORCIO EMDOC
EMDOC
CONSORCIO

2.8. Rendimiento de la plataforma VeriGO MobileID

Existen cuatro formas de medir el rendimiento de VeriGO MobileID:

2.8.1. Rapidez y capacidad de respuesta

La plataforma VeriGO MobileID debe procesar las solicitudes de emisión, autenticar las identidades y responder con credenciales de identidad firmadas rápidamente. La base de datos del sistema backend Veridos está diseñada para ser nativa de la nube, lo que le permite procesar los documentos de identificación digital de manera eficiente en diversas condiciones

2.8.2. Fiabilidad

La plataforma VeriGO MobileID debe funcionar de forma coherente con un mínimo de tiempo de inactividad o errores. Se instalará, supervisará y mantendrá en el mismo sistema informático que el utilizado para la emisión física de tarjetas. Esto garantizará su fiabilidad y disponibilidad.

2.8.3. Precisión

La Plataforma VeriGO MobileID debe identificar correctamente a los individuos y evitar falsos positivos o negativos. La Plataforma VeriGO MobileID propone el uso del principal software de reconocimiento facial para la verificación de la identidad, heredando el rendimiento, la precisión y la coherencia de los resultados de clase mundial.

2.8.4. Experiencia del usuario

La plataforma VeriGO MobileID debe ser fácil de usar y accesible para todos los usuarios previstos.

2.9. Escalabilidad de la plataforma VeriGO MobileID

La escalabilidad es la capacidad de la plataforma VeriGO MobileID para gestionar un crecimiento constante, ya sea en el número de usuarios o en el volumen de transacciones, sin que disminuya el rendimiento.

2.9.1. Aumento de la carga

La plataforma VeriGO MobileID es nativa de la nube y podrá dar cabida a un número creciente de usuarios y transacciones de manera eficiente.

CONSORCIO EMDOC
EMDOC
CONSORCIO

2.9.2. Infraestructura flexible

La plataforma VeriGO MobileID tiene capacidad para ampliarse con la infraestructura subyacente, ya sea a través de la computación en nube o por otros medios.

2.9.3. A prueba de futuro

La Plataforma VeriGO MobileID está diseñada pensando en el crecimiento futuro, tanto en términos de tecnología como de base de usuarios. La plataforma VeriGO MobileID se mantendrá y actualizará como parte de la estructura de mantenimiento anual.

CONSORCIO EMDOC
EMDOC
CONSORCIO

3 Características de la plataforma VeriGO MobileID

3.1. Contenido de esta sección

En esta sección se describen las principales características del detalle de la plataforma VeriGO MobileID. Esta información es útil para explicar cuáles son las funciones prácticas de la plataforma y por qué es importante

3.2. Introducción a las características de la plataforma VeriGO MobileID

Las características de la aplicación están diseñadas para resolver el problema de la verificación de identidades de forma rápida y sencilla. Por su diseño, es fácil de usar, accesible para todos y extremadamente segura.

Cada una de las funciones de la aplicación esta respaldada por el amplio servicio de atención al cliente que ofrece Veridos. Dispone de un sólido servicio de asistencia para responder rápidamente a las consultas, problemas e inquietudes de los usuarios. En concreto, Veridos prestará apoyo a los usuarios durante la incorporación, la resolución de problemas técnicos y la orientación sobre buenas prácticas

Además, todos los usuarios recibirán recursos de formación y documentación. Esto garantiza que puedan utilizar y gestionar eficazmente su perfil en la plataforma VeriGO MobileID. Los usuarios recibirán guías de usuario, tutoriales en video y material educativo.

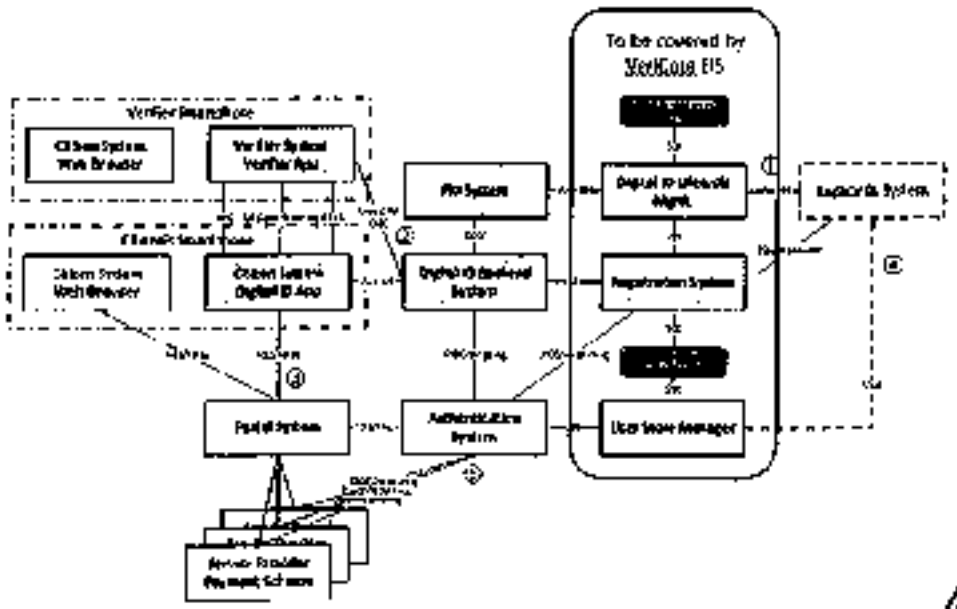


Fig. 1: MID Architecture – Component View

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo

3.3.Características principales

3.3.1. Múltiples identidades con credenciales multifactor

Emisión, almacenamiento y uso seguros de identificación visual, FIDO2, credenciales verificables, push verify, certificados digitales y OTP.

3.3.2. Verificación y autenticación sólidas de la identidad

La autenticación multifactor asegura la privacidad del usuario en línea y fuera de línea. Garantiza que los verificadores puedan confiar en que el usuario es quien dice ser.

3.3 3. Consentimiento del usuario

VeriGO MobileID pone el control en manos del usuario. Ellos deciden qué información privada comparten, dónde se comparte y con quién se comparte.

3.3.4. Propiedad de la identidad

El organismo emisor expide el documento de identificación digital tras su aprobación del mismo modo que lo haría con un documento de identidad físico.

3.3.5. Intención del verificador

El verificador realiza la solicitud de atributos de identidad del usuario. Esto puede hacerse con o sin conexión a Internet. Para fuera de línea, BLE es operativo, y mientras el usuario está conectado en línea, OIDC4VP o REST es operativo.

3.3.6. Gobernanza de la privacidad de los datos

Los datos de los usuarios están protegidos en tránsito y en cada plataforma. Los datos están protegidos al máximo nivel posible, incluso con funciones de elementos seguros en tiempo real.

3.4.Funciones auxiliares de la plataforma VeriGO MobileID

3.4.1. Notificaciones push

VeriGO MobileID abre un canal de comunicación directo entre el organismo emisor y los usuarios de la aplicación a través de notificaciones push. La plataforma VeriGO MobileID envía automáticamente

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo

notificaciones push en determinadas situaciones, como por ejemplo, el perfil de un usuario se retira o caduca, o un administrador cambia la dirección de un usuario.



3.4.2. Gestión de perfiles

Los usuarios de VeriGO MobileID tienen la posibilidad de darse de baja del programa de la Plataforma VeriGO MobileID con dos clics.

Tras pulsar el botón de baja y confirmar su intención de darse de baja del programa, el sistema borra su perfil y el material criptográfico específico del usuario.

En consecuencia, la conexión criptográfica entre el smartphone y la base de datos del sistema backend de Veridos se elimina de forma irreversible. Los usuarios que deseen reactivar su perfil posteriormente podrán volver a inscribirse en el programa de la Plataforma VeriGO MobileID en cualquier momento. Para ello, deberán someterse de nuevo a uno de los procedimientos de inscripción disponibles, ya que la base de datos del sistema backend de Veridos no almacena ningún dato del usuario tras su cancelación.

CONSORCIO EMDOC

3.5.Programa de mantenimiento

El mantenimiento continuo de un sistema de identificación digital es crucial para garantizar su eficacia, seguridad y cumplimiento de las leyes y normativas pertinentes

Entre ellas figuran:

3.5.1. Actualizaciones y parches periódicos del software

Veridos pondrá en marcha un programa para actualizar y parchear periódicamente el software con el fin de protegerlo contra las vulnerabilidades. En concreto, esto incluye actualizaciones del sistema operativo, el software de aplicación y el software de seguridad.

3.5.2. Supervisión continua de la seguridad

Veridos establecerá una supervisión continua de las amenazas y vulnerabilidades de seguridad. Esto incluirá auditorías de seguridad periódicas y la supervisión de las actividades del sistema

3.5.3. Planes de copia de seguridad y recuperación de datos

La plataforma VeriGO Mobile® se instalará en la misma infraestructura informática que la solución principal, lo que garantiza la existencia de sólidos procedimientos de copia de seguridad y recuperación de datos.

3.5.4. Supervisión y optimización del rendimiento

Veridos supervisará continuamente el rendimiento del sistema y aplicará las optimizaciones necesarias. Esto incluye escalar los recursos para satisfacer la demanda, optimizar las bases de datos y mejorar la eficiencia del sistema

3.5.5. Asistencia y formación de usuarios

Se proporcionará asistencia y formación continuas a los usuarios para responder a sus preguntas y problemas. Es esencial que el personal y los usuarios reciban formación periódica sobre las actualizaciones del sistema, las prácticas de seguridad y el cumplimiento de las normas.

CONSORCIO EMDOC
EMDOC
CONSORCIO
SANTO DOMINGO, R.D.

4 La tecnología de la plataforma VeriGO MobileID

4.1. Contenido de esta sección

En esta sección se describe detalladamente la tecnología de la plataforma VeriGO MobileID, incluida la tecnología básica y la patentada. Esta información es útil para explicar cómo funciona la plataforma y lo eficiente, fiable y coherente que es.

4.2. Introducción a la tecnología de la plataforma VeriGO MobileID

La plataforma VeriGO MobileID se basa en tecnología punta para funcionar con el máximo nivel de seguridad. La base de esta plataforma sin fisuras es la base de datos del sistema backend de Veridos, extremadamente segura, que almacena de forma segura los datos personales de cada usuario de la aplicación.

Veridos conecta la plataforma VeriGO MobileID al sistema Vericore ICE Enrollment, responsable del registro biográfico y biométrico. La seguridad de la aplicación y de la base de datos del sistema Veridos minimiza el riesgo de falsificación de documentos. Estas sólidas características de seguridad garantizan que el cliente pueda confiar en la fiabilidad de todo el proyecto.

Debido a la naturaleza flexible del Sistema de Registro Vericore ICE, es posible ampliar una infraestructura existente de la Plataforma VeriGO MobileID para digitalizar una amplia gama de documentos. Más allá de los permisos de conducir digitales, la matriculación de vehículos o los permisos de pesca, convirtiendo así la aplicación en un verdadero monedero digital para el futuro.

Para garantizar un alto nivel de funcionalidad y seguridad, VeriGO MobileID utiliza tecnología propia para conectar la base de datos del sistema backend de Veridos con las partes interesadas:

- Usuarios de la aplicación
- Verificadores físicos (como agentes del orden)
- Verificadores digitales (como un portal de administración electrónica o un sitio web bancario)

4.3. La tecnología fundamental de la plataforma VeriGO MobileID

La verificación de la identidad de los usuarios con soluciones virtuales y digitales requiere mecanismos tecnológicos que se basan en la criptografía.

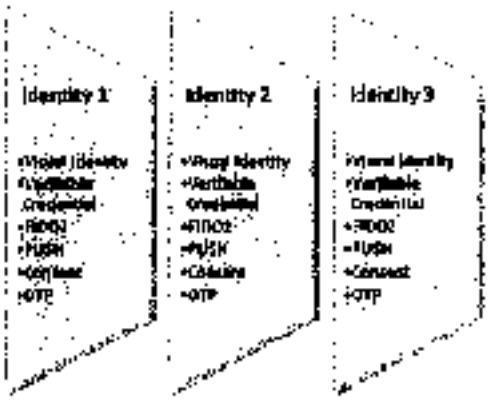
Durante la fase de implementación, una infraestructura de clave pública (PKI) de software suministrada por Veridos proporciona los mecanismos criptográficos esenciales.

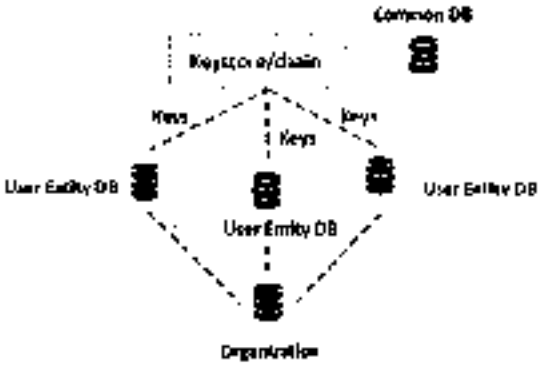
CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo

Para reducir la dependencia del sistema de la infraestructura de servidores subyacente, los sistemas VeriGO MobileID se ejecutan en contenedores Docker.

Veridos ofrece todos los servicios en paquetes que contienen todas las dependencias necesarias. Los procesos establecidos de Veridos garantizan la agilidad y escalabilidad de la plataforma VeriGO MobileID. La capacidad está incorporada para apoyar a los usuarios a medida que aumenta el número.

Es posible alojar y operar la base de datos del sistema backend de Veridos in situ en el centro de datos del cliente o en un entorno basado en la nube. VeriGO MobileID se basa en estándares e interfaces estandarizadas como OpenID Connect (OAuth 2.0) o SAML 2.0.





4.4. Tecnología en la que pueden confiar los verificadores

La tecnología patentada de la plataforma VeriGO MobileID gestiona los datos personales de los usuarios de acuerdo con las normas aplicables (ISO 18013-5 o norma W3C de credenciales verificables). Esto garantiza que los verificadores reciban información auténtica sobre el usuario que desean verificar.

Las bases de datos y la tecnología patentada del sistema VeriGO MobileID Platform establecen procesos y fundamentos de confianza. La facilidad de uso de la aplicación permite a terceros, como bancos, aerolíneas, hoteles, casinos o licorerías, conectarse fácilmente al sistema. Una experiencia fluida con la aplicación significa que es fácil verificar rápidamente la identidad de los usuarios. Cualquier oportunidad de agilizar la interacción entre empresa y cliente es una oportunidad de impresionar al cliente y crear una experiencia positiva. Desde el punto de vista comercial, procesar las interacciones con los clientes sin problemas y con mayor eficiencia ahorra dinero.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo

4.5.Orgullosos de estar a la vanguardia de los avances tecnológicos

Veridos ha demostrado su compromiso de mantenerse a la vanguardia de la tecnología incorporando innovaciones y tendencias emergentes en materia de identidad digital.

Esto incluye mejoras progresivas en áreas como:

- Inteligencia artificial
- Aprendizaje automático
- Biometría avanzada
- Avances en los métodos de autenticación
- Tecnologías de cifrado
- Características de usabilidad.

Veridos comunica el ciclo de vida del producto, incluyendo las fechas de fin de soporte y los planes de actualización o sustitución del producto. Esta transparencia ayudará a BIDMV a planificar el uso a largo plazo de la plataforma VeriGO MobileID.

4.6.Tecnologías utilizadas en la plataforma VeriGO MobileID

Nombres	Acciones
Inquilino a bordo	Proceso de aprovisionamiento gestionado internamente
Microservicio Spring Boot	OpenJDK 8/17 Config-server- añadir o eliminar tenant URI Endpoints- incluir identificador de inquilino
Base de datos: (Compartida)	Postgres v15.1 RLS (Row Level Separation) en la base de datos: Todas las tablas con datos PII o de inquilinos contienen la columna de identificación del inquilino
Protocolos	OIDC, SAMI 2.0, OAuth2.0, LDAP-AD, SCIM 2.0
Credenciales	Credencial verificable, FIDO2, PUSH(Consentimiento), PKI, OTP
Infraestructura	En las instalaciones / AWS en la nube

CONSORCIO EMDOC
EMDOC CONSORCIO
Santo Domingo

5 La seguridad de la plataforma VeriGO MobileID

5.1. Contenido de esta sección

Esta sección describe la seguridad de la plataforma VeriGO MobileID en detalle, incluyendo GDPR y privacidad, encriptación y registro. Esta información es especialmente útil para generar confianza y convencer al cliente de su fiabilidad.

5.2. Introducción a los sistemas de seguridad de la plataforma VeriGO MobileID

La seguridad es la máxima prioridad para Veridos.

Mantener a salvo a los usuarios y sus datos es fundamental, como también lo son unos procesos de seguridad rigurosos en los que los verificadores puedan sentirse seguros. Las bases de datos del sistema backend de Veridos y su tecnología propia se basan en sólidos procesos de seguridad que dan prioridad a la fiabilidad, la protección y la autenticación.

5.3. Mantenimiento de seguridad

La vigilancia de la seguridad es continua. Como parte del soporte y mantenimiento de la plataforma VeriGO MobileID, se proporcionan parches y actualizaciones para hacer frente a las vulnerabilidades. Además, la plataforma VeriGO MobileID se adapta a los cambios en materia de seguridad manteniéndose a la vanguardia de los avances tecnológicos.

Este mantenimiento de la seguridad garantiza que la plataforma VeriGO MobileID siga siendo segura y fiable a lo largo del tiempo. Los expertos e ingenieros de Veridos colaboran activamente con los organismos reguladores pertinentes para mantenerse informados sobre la evolución de los requisitos normativos. La colaboración con las autoridades ayuda al proveedor de soluciones a anticiparse a los cambios en el panorama normativo y a ajustar la plataforma VeriGO MobileID en consecuencia.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo

5.4. Directrices de seguridad de la plataforma VeriGO MobileID

Normas	Acciones
Datos cifrados en tránsito	Activar el cifrado de la capa de transporte TLS 1.3 o TLS 1.2.
SSO MFA y verificación	Habilite la autenticación multifactor: FIDO2, PUSH, PKI, OTP, código QR
Proteger el acceso a aplicaciones y puntos finales	Es obligatorio acceder a todos los puntos finales y a la aplicación utilizando tokens JWT válidos a través de OAUTH o claves de acceso a la API.
Controles de acceso basados en funciones	Aplicar políticas y gobernanza para limitar el acceso de los usuarios en función de la función asignada es fundamental .
Desconfiguración de la seguridad	Aplique las configuraciones sólo después de revisarlas y aprobarlas mediante la comprobación del cumplimiento de la seguridad .
Prevención de la pérdida de datos	Copias de seguridad frecuentes en cintas para mitigar la pérdida de datos y respaldar el BCP (Business Continuity Plan) .
Comprobación de seguridad antes de la implantación	Asegure la infraestructura y la red antes del despliegue : VPN, inicio de sesión con clave SSH.
Registro y control	Habilitar el registro de aplicaciones que ayudaría en caso de compromiso.

5.5. Normas de seguridad de la plataforma VeriGO MobileID

Norma de seguridad	Protocolos
Clave simétrica	AES: 128, 256 Longitudes de clave configurables.
Clave asimétrica	RSA: 2048, 4096 Longitudes de clave configurables. ECC: 256, 384, 521 Longitudes de clave configurables.
Resumen de mensajes	SHA: 256,384, 512 Bits configurables.
mID/mDL Estándar	Permiso de conducir conforme a ISO/IEC 18013-5- ISO.
Código de autenticación del mensaje	HMAC: SHA-256, SHA-384, SHA-512 Bits configurables.
Https seguros	TLS: v1.3 v1.2 están configurados con suites de cifrado fuertes.
Autenticación y verificación multifactoriales	Orden precedente: FIDO2 - PUSH - PKI - OTP - Código QR.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo

5.6. Cifrado de extremo a extremo

Todos los datos transferidos hacia y desde la aplicación son seguros y no pueden ser accedidos por partes no autorizadas, incluyendo Veridos. La aplicación solo recopila y almacena la información esencial necesaria para su funcionamiento, evitando la recopilación innecesaria de datos.

Se facilitan políticas de privacidad transparentes y comprensibles que detallan cómo se utilizan, almacenan y protegen los datos de los usuarios.

- El derecho al olvido: permite a los usuarios que lo soliciten borrar completamente sus datos de la aplicación.
- Dentro de la aplicación, los datos del usuario sólo se almacenan durante el periodo necesario para el fin con el que se recogieron.
- Autenticación de dos factores (2fa): el usuario puede activar esta capa adicional de seguridad más allá del nombre de usuario y la contraseña.

5.7. Seguridad del usuario en la plataforma VeriGO MobileID

5.7.1. Funciones cronológicas

Una medida de seguridad fundamental para los usuarios de la aplicación es la función de cronología. Cada interacción entre el usuario, el verificador, los organismos emisores y otras partes interesadas se registra con la fecha y la hora de la interacción. Este registro electrónico garantiza un alto nivel de control y transparencia para usuarios y verificadores, permitiendo a cada usuario ver qué documentos de identificación ha compartido con qué verificador y cuándo.

5.7.2. Procesos de inscripción sólidos

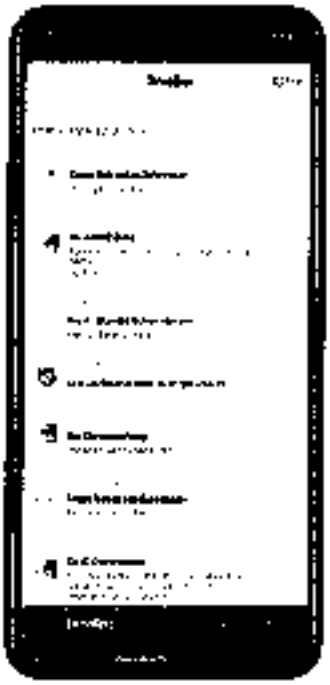
Otro aspecto de seguridad fundamental se encuentra en los procesos de inscripción. Cuando un usuario se inscribe en la plataforma, ya sea en persona o en línea, cada etapa es rigurosamente segura.

Durante el proceso de registro, la aplicación crea un par de claves pública y privada. La aplicación envía la clave pública y el certificado digital correspondiente a la base de datos del sistema backend de Veridos. En este punto, el certificado es firmado por la infraestructura de clave pública (PKI) dentro de la base de datos del sistema backend de Veridos

A partir de ese momento, la aplicación de usuario está conectada criptográficamente a la base de datos del sistema backend de Veridos. En otras palabras, cada vez que los usuarios inician su aplicación de usuario, la base de datos del sistema backend de Veridos puede determinar con precisión con qué smartphone interactúa basándose en un mecanismo criptográfico.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo

Además, sea cual sea el proceso de inscripción por el que opte el usuario, al inscribirse concede varios permisos para el tratamiento de datos y la funcionalidad del smartphone. Entre otras cosas, permite que la aplicación acceda a la función de cámara del smartphone y acepta los términos y condiciones de la aplicación.



5.8. Aprovisionamiento: procesos de inscripción seguros

El aprovisionamiento comprende la inscripción de usuarios para convertirse en usuarios de una VeriGO MobileID, así como la adquisición y almacenamiento reales de un documento móvil por parte del usuario inscrito.

Veridos ofrece a los usuarios varias opciones de inscripción para obtener una VeriGO MobileID. Para la fase inicial, existen dos métodos de inscripción alternativos: inscripción en persona en la autoridad de registro e inscripción en línea. Además, esta sección describe una tercera: un procedimiento de autoinscripción totalmente automatizado. Esta opción será relevante en una posible fase posterior del proyecto.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo

5.9.Tres ejemplos de procesos de inscripción seguros

5.9.1. Ejemplo uno | seguridad de los usuarios: inscripción en persona

Los usuarios que necesiten apoyo adicional en la gestión de procesos tecnológicos pueden inscribirse personalmente en la Plataforma VeriGO MobileID. Estos son los pasos seguros para que un usuario se inscriba en VeriGO MobileID:

- Primer paso

  Los usuarios descargan la plataforma VeriGO MobileID desde App Store, Google Play Store o la tienda pública correspondiente a su smartphone.

- Paso 2

  Los usuarios acuden a la autoridad de registro, donde demuestran su identidad con un documento de identificación físico o digital tradicionalmente aceptado. Los administradores formados de la plataforma VeriGO MobileID verifican los documentos y la identidad del usuario.

- Paso 3

  Los usuarios inician su aplicación de usuario por primera vez y eligen la opción "Inscripción en persona". Aparecerá un código QR de inscripción en su pantalla.

- Paso 4

  El administrador de la plataforma VeriGO MobileID escanea este código QR de inscripción. Esto desencadena un procedimiento de inscripción automatizado.

Veridos recomienda implementar la opción de inscripción en persona en la fase inicial del proyecto de la Plataforma VeriGO MobileID, así como en posibles fases posteriores del proyecto.



5.9.2. Ejemplo dos | seguridad de los usuarios: inscripción en línea

Los usuarios con confianza en la gestión de transacciones en línea pueden inscribirse en línea sin necesidad de asistencia presencial

- Primer paso

Los usuarios descargan la plataforma VeriGO MobileID desde App Store, Google Play Store o la tienda pública correspondiente a su smartphone

- Paso 2

Los usuarios solicitan en línea su inscripción en VeriGO MobileID. Visitan un sitio web de inscripción e introducen una fotografía y su nombre legal completo, fecha de nacimiento y dirección. Una vez registrado en el sitio web, el usuario puede ser localizado en la base de datos del sistema backend de Veridos.

- Paso 3

Se envía un código QR de inscripción a la dirección de correo electrónico o al número de teléfono registrados y verificados del usuario.

- Paso 4

Los usuarios inician su aplicación de usuario por primera vez y eligen la opción "inscripción en línea". Con la cámara de su smartphone, el usuario escanea el código QR de inscripción. De este modo, se inicia un procedimiento de inscripción automático

Veridos recomienda implementar la opción de inscripción en línea en la fase inicial. Su aplicación en fases posteriores del proyecto de la plataforma VeriGO MobileID requiere una evaluación previa de viabilidad. El proceso de inscripción en línea depende del acceso a las direcciones de correo electrónico y/o números de teléfono registrados de los usuarios.

5.9.3. Ejemplo tres | seguridad de los usuarios: autoinscripción totalmente automatizada

Este método de inscripción ofrece a los usuarios una forma muy cómoda de registrarse para obtener una VeriGO MobileID. Esto conlleva un alto nivel de usabilidad, sigue siendo sólidamente seguro y permite aumentar rápidamente el número de usuarios.

- Primer paso

Los usuarios descargan la plataforma VeriGO MobileID desde App Store, Google Play Store o la tienda pública correspondiente a su smartphone.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

- Paso 2

Los usuarios inician su aplicación de usuario por primera vez y eligen la opción "automatricula".

- Paso 3

Mediante la aplicación, los usuarios introducen sus datos personales y cargan una fotografía de un documento de identificación físico. A continuación, la plataforma VeriGO MobileID aplica NFC para leer los datos del chip del documento de identificación físico y verificar su firma digital, o bien la aplicación lee los datos pertinentes mediante OCR (reconocimiento óptico de caracteres) para verificar el documento de identificación

- Paso 4

Los usuarios se toman un selfie a través de la aplicación VeriGO MobileID, que incorpora técnicas de detección de vida. La aplicación compara este selfie con la imagen extraída del documento físico. Si la comparación coincide, se activa el procedimiento de registro automático. El servicio de autenticación de identidad se basa en el SDK iProov de comprobación de vitalidad de la identidad biométrica para detectar cualquier impostor. El verificador facial básico iProov utiliza la tecnología liveness assurance™ para validar la identidad del individuo y proporcionar un nivel de garantía de que la persona es real y auténtica.

5.10. Seguridad del verificador en la plataforma VeriGO MobileID

En toda la sociedad hay infinidad de verificadores, desde agentes de la ley a agentes inmobiliarios o camareros. Para determinar la identidad de un usuario, los verificadores comprueban actualmente las copias físicas de los documentos de identidad. Deben basarse en características físicas específicas, como hologramas y logotipos, para demostrar la autenticidad de un documento de identificación. Los hologramas físicos son un elemento de seguridad eficaz, por lo que su uso está muy extendido.

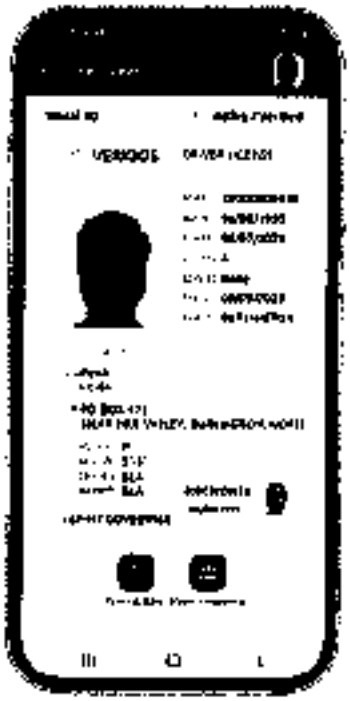
Se espera un uso generalizado de los documentos de identificación digitales en todo el mundo, y la plataforma VeriGO MobileID incorpora eficaces funciones de seguridad. Los procedimientos criptográficos específicos permiten a los verificadores comprobar la integridad y autenticidad de un documento de identificación de forma rápida y segura

Existen elementos de seguridad adicionales para los documentos de identificación digitales, tanto en línea como fuera de línea. Los verificadores pueden confirmar que el documento de identificación de un usuario es auténtico utilizando aplicaciones de verificación. VeriGO MobileID permite tanto a los verificadores como a los usuarios comprobar con confianza la autenticidad de la identificación.

La aplicación de mecanismos criptográficos permite a los verificadores confiar plenamente en los datos mostrados en sus propios teléfonos inteligentes. Los datos transmitidos llevan la firma digital de la base de

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo

datos del sistema backend de Veridos. Las aplicaciones de los verificadores disponen de la clave pública correspondiente, lo que permite un control rápido y seguro de la integridad y autenticidad de los datos.



5.11. Proteja los documentos de identidad de accesos no autorizados

La plataforma VeriGO MobileID protege los documentos de accesos no autorizados incluso si el smartphone se ve comprometido. VeriGO MobileID también implementa el cifrado de extremo a extremo para salvaguardar los documentos almacenados, garantizando que sólo las entidades autorizadas puedan descifrar y acceder a la información.

VeriGO MobileID también implementa el cifrado de extremo a extremo para salvaguardar los documentos almacenados, garantizando que sólo los usuarios autorizados puedan descifrar la información y acceder a ella.

Esto se hace generando una clave privada única en el momento de la provisión de credenciales que se almacena en el almacén seguro de claves del smartphone. La clave pública se comparte con la base de datos del sistema Veridos. El documento de identificación digital, si se aprueba, se encripta utilizando esta clave pública y se envía de vuelta al teléfono inteligente. Sólo puede ser descifrado por la clave privada generada en el momento de la solicitud.

Además, la plataforma VeriGO MobileID ofrece la posibilidad de borrar remotamente el perfil del usuario en caso de robo o pérdida del smartphone. El usuario puede simplemente solicitar el borrado remoto de los datos personales y así se hará.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, D.N.

5.12. Protección contra la falsificación

La plataforma VeriGO MobileID cuenta con varias características inspeccionables digitalmente que ofrecen una gran resistencia a la falsificación de datos.

Como parte de la implementación estándar, los equipos de Veridos llevan a cabo auditorías de seguridad y pruebas de penetración periódicas para identificar y abordar vulnerabilidades en el producto principal y en los módulos personalizados de la plataforma VeriGO MobileID.

Al integrar las medidas mencionadas, Veridos establece un marco global que garantiza la fiabilidad, validez y seguridad de las credenciales digitales a lo largo de todo su ciclo de vida.

5.13. Cumplimiento de las normas

La plataforma VeriGO MobileID cumple las normas y reglamentos pertinentes del sector. Esto incluye normas sobre identidad digital, protección de datos y ciberseguridad. La adhesión a las normas garantiza que la plataforma VeriGO MobileID cumple los requisitos de seguridad y privacidad y es compatible con ecosistemas más amplios. Veridos busca y mantiene activamente certificaciones relevantes relacionadas con la identidad digital y la seguridad. Fomenta las auditorías continuas por parte de entidades externas para validar el cumplimiento y proporcionar garantías a los usuarios y partes interesadas.

Veridos persigue continuamente la implementación, el cumplimiento y la interoperabilidad de las normas ISO/IEC y W3C con múltiples credenciales y carteras. La cartera de productos interna de Veridos impulsa la hoja de ruta de la plataforma hacia una estrategia de componentes cohesiva. A saber, el apoyo a los procesos del cliente, la gestión de las funciones de punto final/suscripción, la elaboración de informes sobre análisis avanzados con la máxima seguridad. Los despliegues de campo, pilotos y prototipos de Veridos utilizan Programas de Adopción Temprana (EAP). Como norma, amplían y diferencian la plataforma a través de un conjunto de integraciones de hardware y software con el cliente y las soluciones de los socios.

Veridos ofrece claridad en relación con sus procesos de desarrollo, la hoja de ruta del producto y las versiones de las funciones. Esta transparencia ayuda a los usuarios a comprender la dirección de la plataforma VeriGO MobileID, las mejoras previstas y las posibles mejoras.

Al hacer hincapié en la asistencia integral, el cumplimiento de las normas y una hoja de ruta clara para el futuro, el proveedor de la plataforma VeriGO MobileID demuestra su compromiso con el éxito de cada proyecto. Esto incluye a sus usuarios, la seguridad de la plataforma VeriGO MobileID y la adaptabilidad a los cambios tecnológicos. Este compromiso es esencial para crear y mantener la confianza de los usuarios, el ecosistema y las partes interesadas.

Veridos reconoce y cumple los requisitos y normas de autenticación de la identificación. Veridos da prioridad al cumplimiento de las normas más recientes del sector. Específicamente, estas incluyen regulaciones de protección de datos como GDPR y cumplirán con todos los requisitos legales y éticos.

CONSORCIO EMDOC
EMDOC CONSORCIO
Santo Domingo, R.D.

5.13.1. Cumplimiento de las normas internacionales

La plataforma VeriGO MobileID estará en consonancia con las normas internacionales pertinentes y con algunas normas regionales, entre las que se incluyen:

- Certificación de la norma ISO/IEC 18013-5 sobre permisos de conducción móviles
- Cumplimiento de la norma ISO/IEC 18013-7 sobre permisos de conducción móviles y otros mDoc (por ejemplo, mVR).
- Cumplimiento de la norma del W3C sobre credenciales verificables

Con el fin de satisfacer los requisitos más recientes y pertinentes de los clientes de la UE, se garantiza el cumplimiento de la normativa de la UE recientemente introducida en el ámbito de la identidad digital:

- Alto nivel de garantía de seguridad e integridad de los datos personales
- Arquitectura compatible con EUDI Wallet ARF
- Componentes de arquitectura conformes con ISO/IEC 18013-/5/7
- Compatibilidad con los protocolos OID4VC y OID4VP.
- Soporte para modelos de confianza centralizados y descentralizados.
- Compatibilidad con los tipos y formatos de credenciales verificables definidos en el capítulo siguiente.
- Apoyo a distintos tipos de procedimientos de incorporación (a distancia o en persona)
- Arquitectura de soluciones abierta y modular
- Solución desplegable in situ o en nubes privadas o públicas.
- Inicio de sesión único

5.13.2. Tipos y formatos de credenciales verificables

Según la normativa eIDAS 2.0, todas las credenciales verificables emitidas por una solución de identidad digital pueden agruparse en tres grandes grupos:

- Datos de identificación de la persona (PID)
- Atestación electrónica cualificada de atributos (QEAA)
- Atestación electrónica de atributos (AEA)

Para Veridos Digital Icentity Solution, los tipos más importantes de credenciales verificables son los emitidos por las autoridades gubernamentales, es decir, los PID y los QEAA. Por lo tanto, Veridos Digital Identity Solution admite la emisión de este tipo de credenciales verificables.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santiago

5.13.3. Datos de identificación de la persona (PID)

Los Datos de Identificación Personal (PID) son la forma más importante y segura de credenciales verificables. Los PID son expedidos directamente por las autoridades gubernamentales y sirven como la prueba más fundamental de la identidad de una persona. Los PID son credenciales emitidas por el gobierno que vinculan a una persona con su estatus legal.

En el caso de las personas jurídicas, los PID suelen denominarse LPID (Legal Person Identification Data, datos de identificación de la persona jurídica), que son cruciales para interacciones seguras y verificadas entre servicios públicos y privados.

Ejemplos:

- documento de identificación móvil (mID) expedido por el gobierno, credencial digital de viaje (DTC), permiso de conducir móvil (mDL).
- LPID - certificado de registro de empresa que acredita la personalidad jurídica.

5.13.4. Atestación electrónica cualificada de atributos (QEAA)

La atestación electrónica cualificada de atributos (QEAA) se utiliza en entornos bien regulados. Las QEAA sólo pueden ser emitidas por un proveedor de servicios de confianza cualificado (QTSP). Las QEAA tienen un efecto legal equivalente al de las atestaciones en papel y se utilizan en casos en los que el cumplimiento y la confianza son fundamentales, como la sanidad, las finanzas o los servicios gubernamentales.

Ejemplos.

- Licencias médicas o jurídicas, certificados de contabilidad o credenciales de enseñanza.
- Certificados de nacimiento, matrimonio o adopción.
- Carnés de estudiante o becario.
- Licencias que autorizan a las empresas a operar legalmente en jurisdicciones específicas
- Documentos que autorizan a alguien a actuar en nombre de otro en asuntos jurídicos o financieros.
- Títulos de propiedad que verifican la titularidad de los bienes inmuebles

5.13.5. Atestación electrónica de atributos (AEA)

Una organización emite un certificado electrónico de atributos (EAA) que verifica información específica sobre una persona. Las EAA se utilizan en entornos no regulados, donde no existen normas legales estrictas como

CONSORCIO EMDOC
Santo Domingo, R. D.

el caso de las credenciales emitidas por el gobierno. Las EAA son fáciles de emitir y constituyen una buena solución para las organizaciones que necesitan una forma sencilla de interactuar con clientes o empleados.

Ejemplos:

- Entradas para actos sociales
- Tarjetas de fidelización de clientes
- Tarjetas de acceso para empleados
- Tarjetas de afiliación
- Billetes de transporte público

5.13.6. Formatos de credenciales verificables

Los formatos normalizados para la emisión de PID y QEAA compatibles con la solución Veridos Digital Identity son los siguientes:

- mDoc/mDL (definido por ISO/IEC 18013-5/7)
- Modelo de datos de credenciales verificables 2.0 del W3C

CONSORCIO EMDOC

6 Integración de la plataforma VeriGO MobileID

6.1. Contenido de esta sección

En esta sección se describen los métodos que Veridos propone para poner en marcha, gestionar y mantener el proyecto, en consonancia con los procesos existentes del cliente. Al describir los detalles exactos, el cliente puede estar seguro de la capacidad y atención al detalle de Veridos.

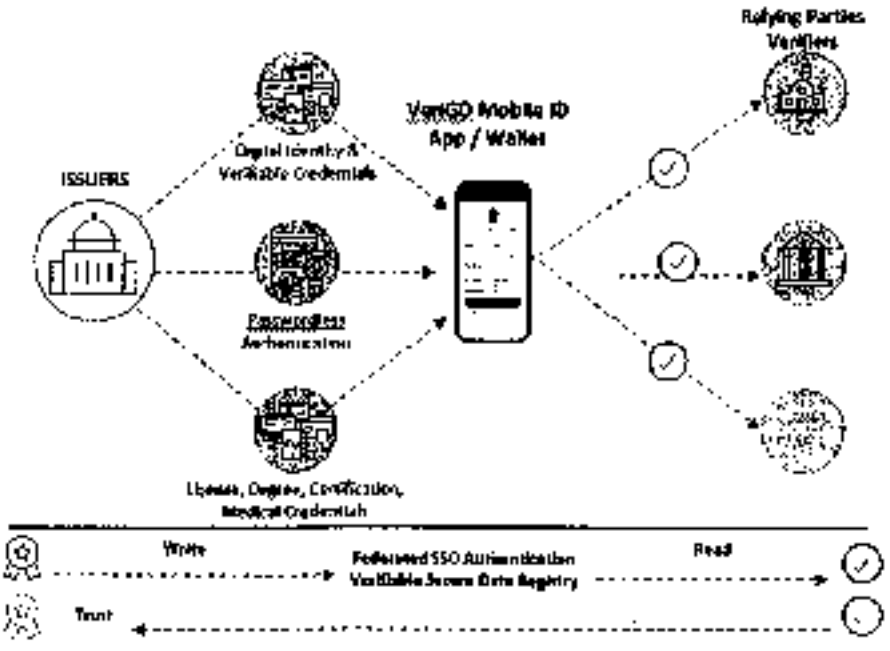
6.2. Introducción a la integración de la plataforma VeriGO MobileID

La plataforma VeriGO MobileID ofrece una asistencia completa, garantizando una integración perfecta y un rendimiento coherente en diversas plataformas y entornos.

Las capacidades de integración son la posibilidad de conectar y automatizar sistemas y procesos en toda una organización o infraestructura nacional. Es decir, la capacidad de intercambiar datos, desencadenar eventos y orquestar flujos de trabajo.

Las capacidades de integración son esenciales para la transformación digital, ya que permiten a las organizaciones acabar con los silos, agilizar las operaciones y mejorar la eficiencia. Entre los beneficios se incluyen el aumento de la productividad, la reducción de costes, la mejora de la calidad de los datos, la mejora de la agilidad y la mejora de la experiencia de clientes y socios.

A la hora de ofrecer capacidades de integración, es importante tener en cuenta el público objetivo, la propuesta de valor, el modelo de entrega y el modelo de precios del cliente :



CONSORCIO EMDOC
EMDOC
CONSORCIO

6.3.Tipos de capacidades de integración

6.3.1. Integración de datos

La capacidad de intercambiar datos entre distintos sistemas y aplicaciones

6.3.2. Integración de procesos

Capacidad para automatizar y orquestar procesos empresariales en múltiples sistemas y subsistemas.

6.3.3. Integración de aplicaciones

La capacidad de conectar e integrar distintas aplicaciones.

6.3 4. Integración API

La capacidad de exponer y consumir API.

6.3.5. Integración de microservicios

La capacidad de conectar e integrar microservicios.

6.4.Tecnologías de Integración

Existen diversas tecnologías de integración, a saber:

6.4.1. Plataforma de integración como servicio (iPaaS

Una plataforma basada en la nube para integrar aplicaciones y datos

6.4.2. Plataforma de gestión de API

Una plataforma para gestionar y exponer API.

6.4.3. Arquitectura de microservicios

Un estilo arquitectónico promueve el desarrollo de servicios pequeños, independientes y autónomos que pueden integrarse fácilmente.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo

6.5. Componentes clave de integración de la plataforma VeriGO MobileID

La integración con diversos organismos y servicios, permitiendo a los usuarios acceder a una amplia gama de servicios a través de su identidad digital se establecen a través de una incorporación de la Plataforma VeriGO MobileID. Esta integración incluye el acceso a herramientas e interfaces como:

6.5.1. Biometría

Los métodos de autenticación del teléfono inteligente, como la huella dactilar o el reconocimiento facial, para el acceso seguro al monedero de identidad móvil, son nativos de la aplicación

6.5.2. Pruebas de conocimiento-cero

Las tecnologías de preservación de la privacidad garantizan que los datos personales sólo se compartan cuando el usuario lo necesite. Por su diseño, la plataforma VeriGO MobileID no requiere contraseña nativa, PKI, consentimiento ni fricción.

6.5.3. Imágenes Dockerizadas

El despliegue local puede realizarse rápidamente con imágenes dockerizadas e incluiría las mejores prácticas de confianza cero. El despliegue local se configurará junto con el equipo de Veridos. Esto incluye la configuración inicial de los servidores de la plataforma, los servidores de redundancia, HSM para PKI y el equipo de red relacionado.

6.5.4. Herramientas de control

Se configurarán con la orientación de cliente. De este modo se garantiza un seguimiento preciso de la salud y el rendimiento de la plataforma y las aplicaciones.

6.6. Planificación de la integración de la plataforma VeriGO MobileID

El objetivo de la fase de planificación es comprender plenamente los requisitos específicos del proyecto y el entorno en el que Veridos desplegará e integrará la plataforma VeriGO MobileID.

Esta tarea comenzará con un análisis de las leyes, políticas, procedimientos y normas aplicables. Los ingenieros y expertos de Veridos examinarán las infraestructuras existentes y colaborarán estrechamente con todas las partes interesadas posibles, a fin de reunir los requisitos para el proyecto específico.

CONSORCIO EMDOC
EMDOC
CONSORCIO

6.7.Diseño de la integración de la plataforma VeriGO MobileID

Veridos diseña la aplicación basándose en el resultado de la fase de planificación. Un equipo formado por diferentes expertos en TI -incluidos integradores de sistemas, arquitectos de seguridad y arquitectos de software- evaluará la fase de planificación. A continuación, preparan el sistema de la plataforma VeriGO MobileID. Se tendrán muy en cuenta todos los aspectos del diseño, desde la arquitectura hasta la accesibilidad, la seguridad y la experiencia del usuario.

6.8.Desarrollo de la integración de la plataforma VeriGO MobileID

Los ingenieros y expertos de Veridos organizarán todo el desarrollo de acuerdo con un ciclo de vida de desarrollo de software ágil y se adherirán al marco scrum. Veridos tiene un historial probado de combinación de metodologías ágiles de desarrollo de software con procesos de contratación pública.

Como proveedor de soluciones de alta seguridad, el más alto nivel de seguridad es fundamental para todos los productos de Veridos. Veridos ha adaptado el marco general scrum para integrar la seguridad en los procesos de desarrollo de Veridos. La plataforma VeriGO MobileID se desarrolla según el principio de "seguridad y protección por defecto". Cada equipo scrum incluye un representante de seguridad que aplica herramientas como el modelado de amenazas o el análisis de riesgos para examinar todos los elementos del sprint-backlog desde el punto de vista de la seguridad.

6.9.Pruebas de Integración de la plataforma VeriGO MobileID

Para garantizar un funcionamiento sin problemas, todos los productos de software de Veridos se prueban en varias fases. Siguiendo un camino hacia el despliegue continuo, una gran parte del software se prueba automáticamente con cada confirmación en el sistema de control de versiones. Además, Veridos también realiza algunas pruebas exploratorias y de UX manuales antes del lanzamiento de un software.

Las pruebas incluyen:

- Pruebas de conformidad para garantizar que el sistema VeriGO MobileID Platform cumple las normas ISO/IEC 18013-5 / 18013-6.
- El sistema de integración continua ejecuta pruebas unitarias y de integración automatizadas con cada compilación.
- Las pruebas de humo según un plan de pruebas definido incluyen ensayos sencillos de la aplicación para detectar errores simples pero evidentes de forma rápida y eficaz.
- Las pruebas de rendimiento garantizan que la aplicación responda en el límite de tiempo predefinido.

CONSORCIO EMDOC
EMDOC
CONSORCIO

- Las pruebas de estrés verifican que la aplicación responderá adecuadamente con muchos usuarios y actividades sucediendo simultáneamente.

- Las pruebas de extremo a extremo confirman que la aplicación interactúa correctamente con los demás sistemas y el usuario final. Durante estas pruebas, ingenieros y expertos utilizan un conjunto controlado de transacciones y publican los datos de prueba antes de la prueba junto con los resultados esperados.

- Las pruebas de penetración son un intento de evaluar la seguridad de una infraestructura informática tratando de explotar vulnerabilidades de forma segura. Estas vulnerabilidades pueden existir en sistemas operativos, servicios y fallos de aplicaciones, configuraciones inadecuadas o comportamientos arriesgados de los usuarios finales.

- Las pruebas de recuperación en caso de catástrofe garantizan la existencia de procedimientos adecuados para restaurar el sistema en caso de catástrofe.

- Despliegue de la integración de la plataforma VeriGO MobileID Tras crear y probar con éxito la aplicación, el software resultante se despliega en todos los entornos de prueba y de ensayo. Si las pruebas exploratorias arrojan un resultado positivo, el software se despliega en el sistema de producción. Todos los pasos de este proceso, excepto la fase de pruebas exploratorias, se realizan de forma totalmente automatizada y sin interacción humana.

6.10. Diversidad en los datos de formación

Veridos revisa y utiliza modelos de aprendizaje automático que pueden adaptarse con el tiempo a la evolución de las amenazas y los patrones de ataque. Veridos se asocia con proveedores de algoritmos biométricos de primer nivel que entrenan los modelos en diversos conjuntos de datos para reducir los sesgos y los actualizan periódicamente para estar al día de las nuevas tendencias. Veridos emplea conjuntos de datos y pruebas independientes para garantizar que los algoritmos integrados están diseñados para detectar y mitigar los sesgos en los procesos de verificación de identidad.

El equipo de Veridos audita y comparte regularmente los resultados y proporciona información a sus proveedores de soluciones biométricas para perfeccionar estos algoritmos con el fin de abordar posibles sesgos en la comparación de rostros y la toma de decisiones durante la adjudicación humana

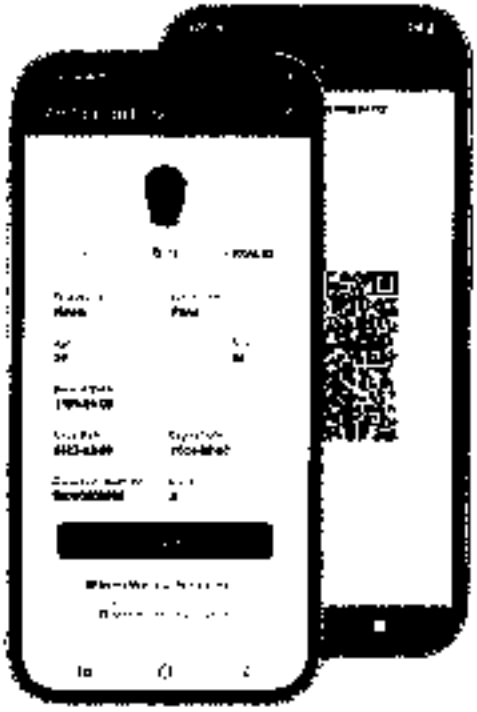
Los proveedores de soluciones biométricas integradas de Veridos garantizan que los datos de entrenamiento utilizados para los modelos de aprendizaje automático sean diversos y representativos de diferentes grupos demográficos. Esto ayuda a minimizar los sesgos y garantiza que el sistema sea justo e inclusivo para todos los usuarios. El proveedor de soluciones biométricas también realiza auditorías periódicas de los datos de formación para identificar y rectificar cualquier sesgo que pueda haberse introducido inadvertidamente. Esto es esencial para mantener la equidad y la precisión en el sistema de credenciales de identificación digital.

CONSORCIO EMDOC
EMDOC
CONSORCIO
S. Damian

7 Casos prácticos Usuarios de la plataforma VeriGO MobileID

7.1.Contenido de esta sección

Esta sección ilustra los usos y beneficios de la Plataforma VeriGO MobileID con ejemplos de funcionalidad de la "vida real". Esta sección pretende que todos los aspectos del uso y las ventajas de utilizar la Plataforma VeriGO MobileID sean claros, directos y accesibles para todos. Los estudios de casos tienden a ser persuasivos debido al lenguaje descriptivo y coloquial que garantiza que el mensaje se comunique con claridad.



7.2.Caso práctico 1

Un usuario viaja en su coche cuando un agente de policía le da el alto para realizar un control estáncar en carretera

La oficina de policía formula las preguntas reglamentarias y pide al usuario que demuestre su identidad. A pesar de encontrarse en una zona con poca señal y sin wi-fi, el usuario puede acceder a la plataforma VeriGO MobileID sin conexión.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo

El agente de policía escanea la aplicación del usuario para averiguar su identidad. En unos segundos, todo está confirmado y verificado. Una vez que la oficina de policía ha completado el control en carretera, el usuario se pone rápidamente en camino.

7.3. Caso práctico 2

Un usuario necesita utilizar un servicio local de coche compartido. Puede crear un perfil con el servicio de coche compartido, verificar su identidad y confirmar sus cualificaciones de conducción rápidamente con la aplicación VeriGO MobileID Platform.

Al acercarse al coche disponible más cercano, el usuario puede utilizar la aplicación VeriGO MobileID Platform para autenticar el viaje. El usuario confirma en la aplicación que da su consentimiento para que el servicio de car sharing acceda a sus datos. Con la tecnología biométrica, el servicio de car sharing confirma la identidad del usuario y confirma la reserva del coche.



7.4. Casos de usuarios adicionales

En el anexo encontrará una amplia gama de casos de uso

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo

8 Preparar para el futuro la plataforma VeriGO MobileID

8.1. Contenido de esta sección

Esta sección ilustra los usos futuros de la plataforma VeriGO MobileID y señala las oportunidades que tiene el cliente para desarrollar y personalizar la tecnología. Amplía las funciones ya extremadamente útiles y ofrece al cliente la oportunidad de obtener un rendimiento óptimo de la inversión.

8.2. Oportunidades ilimitadas

A medida que las transacciones remotas y virtuales se sistematizan cada vez más, aumenta la necesidad de oportunidades digitales para la verificación de la identidad. Los usuarios de todo el mundo utilizarán plataformas como VeriGO MobileID varias veces al día en su vida cotidiana, y podrán añadir varios documentos a su monedero digital

Veridos tiene previsto ampliar la funcionalidad de la plataforma VeriGO MobileID para maximizar el impacto potencial para los usuarios.

8.3. Herramienta de comunicación

Mediante las notificaciones push, el sistema permitirá a los organismos emisores redactar mensajes específicos y enviarlos a usuarios individuales, a un grupo de usuarios o a todos los usuarios de VeriGO MobileID.

Esta funcionalidad también puede utilizarse para anuncios, recordatorios y actualizaciones. Por ejemplo:

- Un administrador puede enviar notificaciones push a un usuario concreto para recordarle una cita con un departamento gubernamental pertinente.
- Un administrador puede enviar una alerta meteorológica a todos los usuarios registrados en una región determinada.
- Un administrador puede enviar una actualización a todas las personas mayores de 50 años en relación con un chequeo médico.

8.4. Herramienta de administración

La plataforma VeriGO MobileID permitirá a los usuarios renovar y actualizar documentos de identidad importantes dentro de la aplicación. Por ejemplo:

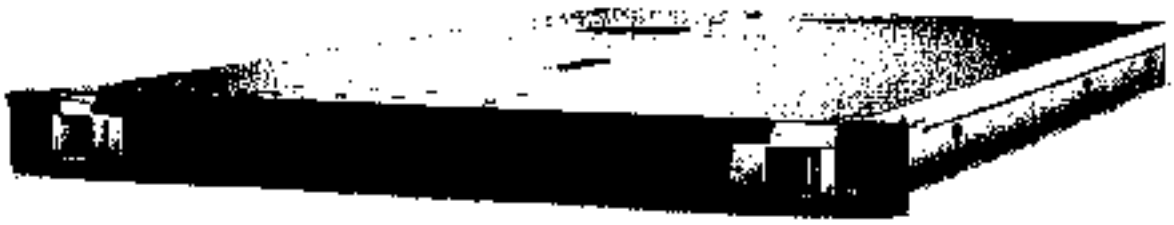
- Actualizar su nueva dirección para el documento nacional de identidad
- Denunciar la pérdida o el robo de un documento de identidad
- Renovar el permiso de conducir

CONSORCIO EMDOC

Traducido del inglés al español - www.onlinedoctranslator.com

HPE GreenLake

HPE ProLiant DL360 Gen11



Qué hay de nuevo

- Equipado con procesadores escalables Intel® Xeon® de cuarta generación que admiten hasta 64 núcleos y 385 W, y 16 DIMM por zócalo para hasta 8 TB de memoria DDR5 de alto ancho de banda de hasta 5600 MHz
- 16 DIMM por procesador para hasta 8 TB de memoria DDR5 total por servidor con mayor rendimiento, compatibilidad con memoria de alto ancho de banda (HBM) y menores requisitos de energía.
- Velocidades de transferencia de datos aceleradas y velocidades de red más altas desde el bus de expansión serie PCIe Gen5, con hasta 2 ranuras PCIe Gen5 x16 y 2 OCP.
- Incluye el nuevo software de administración de servidores HPE Integrated Lights Out 6 (iLO 6) que le permite configurar, monitorear y actualizar de forma segura sus servidores HPE ProLiant Gen11 sin problemas, desde cualquier lugar.
- Admite hasta 3 GPU de ancho único (SW) para acelerar cargas de trabajo gráficas intensas.
- Admite módulos de refrigeración líquida para puntos de diseño térmico (TDP) más altos.

Descripción general

¿Está buscando una solución escalable y con gran capacidad informática para la nube híbrida u otras cargas de trabajo de datos en un entorno virtualizado y en contenedores?

El servidor HPE ProLiant DL360 Gen11 es una solución 1U 2P optimizada para rack que ofrece un rendimiento informático excepcional, una velocidad de transferencia de datos de alta velocidad mejorada y una profundidad de memoria con capacidad informática 2P.

Equipado con procesadores escalables Intel® Xeon® de 4.ª y 5.ª generación con hasta 64 núcleos, 8 TB de memoria y 20 unidades EDSFF, así como un mayor ancho de banda de memoria y E/S PCIe Gen5 de alta velocidad, el servidor HPE ProLiant DL360 Gen11 es una solución perfecta para automatización de diseño electrónico (EDA), CAD y VDI.

El servidor HPE ProLiant 360 Gen11 está diseñado para optimizar la TI con una experiencia operativa en la nube, seguridad integrada y rendimiento optimizado para cargas de trabajo que impulsan su negocio.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

Características

Experiencia operativa intuitiva en la nube: simple, de autoservicio y automatizada

Los servidores HPE ProLiant DL360 Gen11 están diseñados para su mundo híbrido. Los servidores ProLiant DL360 Gen11 cuentan con procesadores Intel® Xeon® de cuarta y quinta generación y simplifican la forma en que controla la computación de su empresa, desde el borde hasta la nube, con una experiencia operativa en la nube.

Transforme las operaciones controlables y ahorre con su equipo pasando de lo reactivo a lo predictivo con visibilidad y conocimientos globales a través de una consola de automatización.

Automatice las tareas para lograr eficiencias en la implementación, escalabilidad instantánea y soporte simplificado y administración del ciclo de vida para reducir y evitar las ventanas de mantenimiento.

Las operaciones automatizadas de autoservicio están habilitadas e integradas en todos los servidores HPE ProLiant Gen11, ya sea que se consuman como una experiencia basada en la nube con HPE GreenLake o mediante herramientas tradicionales de configuración y despliegue.

Simplifique y proteja la gestión de servidores desde el borde hasta la nube con HPE GreenLake para Compute Ops Management. HPE GreenLake para Compute Ops Management es una experiencia de gestión inteligente como servicio que ofrece mayor simplicidad, agilidad y velocidad en todo su panorama informático, a prácticamente

Seguridad confiable por diseño: intransigente, fundamental y protegida

El servidor HPE ProLiant DL360 Gen11 utiliza HPE Silicon Root of Trust, el enfoque fundamental de seguridad de HPE que proporciona una arquitectura de confianza cero a nivel de silicio y garantiza que todo el firmware esencial del servidor esté libre de malware o código comprometido.

Equipado con procesadores escalables Intel® Xeon® de 4ª y 5ª generación, aquellas funciones de seguridad asistidas por hardware y software, incluidas Intel® Software Guard Extensions e Intel® Boot Guard, que ayudan a proteger la base del hardware del servidor sobre la que se ejecutan las aplicaciones críticas y protegen mejor los datos en memoria.

Los servidores HPE ProLiant Gen11 protegen continuamente los servidores en tiempo real al proporcionar una detección rápida de servidores con seguridad comprometida, incluso hasta el punto de no permitir el arranque si se detecta código malicioso, y bloqueando los servidores en el borde con certificados IDevID instalados de forma predeterminada.

Los servidores HPE ProLiant Gen11 brindan recuperación automatizada de un evento de seguridad, incluida la restauración del firmware validado y facilitan la recuperación del sistema operativo, las aplicaciones y los componentes de datos, lo que proporciona una ruta rápida para que un servidor vuelva a estar en línea y a sus operaciones normales.

Integrado en los servidores Hewlett Packard Enterprise, HPE Integrated Lights-Out 6 (iLO 6) es una inteligencia central exclusiva que monitorea el estado del servidor, proporcionando los medios para generar informes, administración continua, alertas de servicio y administración local o remota para identificar y resolver problemas rápidamente.

Rendimiento optimizado para sus cargas de trabajo aceleradas, abiertas y eficientes

El servidor HPE ProLiant DL360 Gen11 es una excelente opción para EDA, CAD, CDN, cargas de trabajo de virtualización de uso general y unificadas, así como análisis de video inteligentes y plataformas SDS y convergentes que requieren una mayor densidad informática con funciones integradas, seguridad y flexibilidad.

Aproveche el mayor rendimiento de su computadora. El servidor HPE ProLiant DL360 Gen11 funciona con procesadores escalables Intel® Xeon® de cuarta y quinta generación con tecnología de proceso de nueva generación que admite hasta 64 núcleos, 3 [illegible] y hasta [illegible]

El servidor HPE ProLiant DL360 Gen11 proporciona velocidades de transferencia de datos avanzadas y mayores velocidades de red desde el bus de expansión PCIe Gen5, con hasta 8 ranuras x16 PCIe Gen5 y 2 ranuras OCP para mejorar el rendimiento de E/S y reducir la latencia.

El servidor proporciona 16 DIMM por procesador para hasta 8 TB de memoria DDR5 en total con mayor ancho de banda de memoria y rendimiento, y menor consumo de energía. Compara

CONSORCIO EMDOC
EMDOC

requisitos.

El servidor HPE ProLiant DL380 Gen11 proporciona información operativa en tiempo real sobre el rendimiento del servidor, además de recomendaciones para ajustar la configuración del BIOS y personalizar reglas de recopilación empresariales. Como antes

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

Especificaciones técnicas — HPE ProLiant DL360 Gen11

Tipo de procesador	Intel®
Familia de procesador	Procesadores escalables Intel® Xeon® de 3ª generación; procesadores Intel® Xeon® de 4ª generación
Número de procesadores	1 o 2
Núcleos de procesador admitidos	Hasta 40 núcleos, dependiendo del procesador.
Caché de procesador	12 - 300 MB, dependiendo del procesador
Velocidad de procesador	3.9 GHz, máximo según procesador.
Tipo de bahías de unidades	Opciones de chasis de unidades de factor de forma SFF (2,5") admiten hasta 40 unidades SFF con 2 procesadores; admiten hasta 20 unidades SFF con 1 procesador. Opciones de chasis de unidades de factor de forma LFF (3,5") admiten hasta 12 unidades LFF con 2 procesadores; admiten hasta 4 unidades LFF con 1 procesador. Opciones de chasis de unidades de factor de forma EDSFF admiten hasta 10 unidades EDSFF con 2 procesadores; admiten hasta 4 unidades EDSFF con 1 procesador. Para obtener descripciones detalladas consulte Quickspecs.
Ranuras de expansión	Máximo 3 ranuras PCIe Gen5 y máximo 2 ranuras OCP 3.0 PCIe5. Para obtener descripciones detalladas consulte Quickspecs.
Memoria máxima	4.0 TB con DCMM, cuando está equipado con 256 GB DDR5
Ranuras de memoria	16 ranuras DIMM de 288 clavijas
Tipo de memoria	Memoria inteligente HPE DDR5
Funciones de protección de memoria	Modo chip HPE Fast Fault Tolerant Memoria ECC avanzada Memoria adicional en línea Memoria reflejada
Una unidad óptica	Opcional: unidad digital HPE SATA DVD-RW de 9,5 mm; unidad HPE Mobile USB BD-RW.
Controladores de almacenamiento	Hasta 4 controladores de almacenamiento Smart Array Gen11 en una variedad de configuraciones, incluidos HBA, controlador de puertos, unidades de cinta y Hardware de RAID (compatible con

Para obtener información técnica adicional, modelos disponibles y opciones, consulte las QuickSpecs

Servicios HPE

No importa en qué etapa de su viaje de transformación se encuentre, puede contar con los servicios HPE para brindarle la experiencia que necesita cuándo, dónde y cómo la necesita. Desde la estrategia y la planificación hasta la implementación, las operaciones en curso y más, nuestros expertos pueden ayudarle a hacer realidad sus ambiciosos objetivos.

Servicios de consultoría

Los expertos pueden ayudarle a trazar su camino hacia la nube híbrida y optimizar sus operaciones.

Servicios gestionados

HPE ejecuta sus operaciones de TI, brindándole un control unificado para que pueda concentrarse en la

Innovación. Servicios operativos

Optimice todo su entorno de TI e impulse la innovación. Administre las tareas operativas de TI diarias mientras libera tiempo y recursos valiosos.

- Servicio HPE Complete Care, un servicio modular diseñado para ayudar a optimizar todo su entorno de TI y cubrir resultados de TI y objetivos comerciales acordados. Todo entregado por un equipo asignado de expertos de HPE
- HPE Tech Care Service, la experiencia de servicio operativo para tecnología HPE. El servicio brinda acceso a expertos en productos especializados, una experiencia digital impulsada por IA y orientación técnica general para ayudar a reducir el riesgo y buscar formas de hacer las cosas mejor.

Servicios de puesta en marcha

Aborde las necesidades específicas de su proyecto de implementación de TI con servicios de implementación y gestión de proyectos personalizados.

Servicios educativos de HPE

Capacitación y certificación diseñadas para profesionales de TI y negocios en todas las industrias. Cree rutas de aprendizaje para ampliar sus conocimientos de una manera específica. Programe la capacitación de la manera que mejor funcione para su negocio con opciones flexibles de aprendizaje continuo.

La opción de Retención de Retención de medios defectuosos (DMR), no aplica sobre discos o unidades SSD. Para elegibilidad, comuníquese con Hewlett Packard Enterprise dentro de un mes del Aprovisionamiento. La garantía integral de materiales defectuosos (CDMR) le permite conservar todos los componentes de retención de datos.

HPE GreenLake

La plataforma de borde a nube HPE GreenLake es la oferta como servicio líder en el mercado de HPE que lleva la experiencia de la nube a aplicaciones y datos en todas partes (centros de datos, nubes múltiples y bordes) para un modelo operativo unificado, total y completamente gestionado en un modelo de pago por uso.

Si buscas más servicios, como **Soluciones de financiación de TI**, explóralos aquí.

Explore HPE GreenLake

Para la versión más reciente de este documento, visite nuestro sitio web de HPE en hpe.com

Póngase en contacto con nosotros

Chat now (sales)

Call now

Buy now

Share now

Get updates

© Copyright 2024 Hewlett Packard Enterprise Development LP. La información contenida en este documento está sujeta a cambios sin previo aviso. Las únicas garantías para productos y servicios de Hewlett Packard Enterprise se establecen en las declaraciones de garantía expresa que acompañan a dichos productos y servicios. Nada de lo aquí contenido debe interpretarse como una garantía adicional. Hewlett Packard Enterprise no se responsabiliza de errores técnicos o editoriales ni de omisiones contenidos en el presente documento.

Intel y Xeon son marcas comerciales de Intel Corporation y sus filiales en los Estados Unidos y otros países.

Las marcas y logotipos que aquí aparecen son propiedad de sus respectivos propietarios y se utilizan únicamente con fines informativos.

Java es una marca registrada de Oracle y/o sus filiales.

La imagen puede diferir del producto real.
PSNH1HR9665ESMXOEM, febrero de 2024

Hewlett Packard Enterprise

CONSORCIO EMDOC
EMDOC
Santo Domingo, R.D.

Traducido del inglés al español - www.onlinedoctranslator.com

318

Ficha de datos

HPE GreenLake

HPE ProLiant DL380 Gen11



Qué hay de nuevo

- Equipado con procesadores escalables Intel® Xeon® de cuarta y quinta generación con tecnología de próxima generación que ofrecen hasta 64 núcleos a 350 W y 16 DIMM para memoria DDR5 a velocidades de hasta 5600 MHz.
- La compatibilidad con hasta 8 TB de memoria DDR5 local con 16 canales DIMM por procesador ofrece un mayor rendimiento, menores requisitos de energía y compatibilidad con memoria de alto ancho de banda (HBM).
- Compatibilidad con PCIe Gen5, lo que proporciona el ancho de banda mejorado, velocidades de señalización de datos avanzadas y mejores mecanismos de reconocimiento de errores para PCIe Gen5.
- Incluye el nuevo software de gestión de servidores HPE Integrated Lights-Out 6 (iLO 6).

Descripción general

¿Está buscando una solución de servidor escalable de doble socket para impulsar el análisis de datos o cargas de trabajo de nube híbrida?

El servidor HPE ProLiant DL380 Gen11 es una solución 2U 2P escalable que ofrece un rendimiento informático excepcional, densidad de memoria con escalabilidad y velocidad de transferencia de datos de alta velocidad para ejecutar sus aplicaciones más exigentes.

Equipado con procesadores escalables Intel® Xeon® de 4.ª y 5.ª generación con hasta 64 núcleos, 8 TB de memoria y 20 unidades EDSFF, así como un mayor ancho de banda de memoria y E/S PCIe Gen5 de alta velocidad, el servidor HPE ProLiant DL380 Gen11 es una solución perfecta para el almacenamiento definido por software, la transcodificación de vídeo y aplicaciones virtualizadas.

El servidor HPE ProLiant DL380 Gen11 está diseñado para optimizar la TI con una experiencia operativa en la nube, seguridad integrada,

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

[redacted]

que le permite configurar, monitorear y actualizar de forma segura sus servidores de HPE ProLiant Gen11 sin problemas y desde cualquier lugar.

- Admite opciones de arranque BOSS-S2 desde cualquier ubicación y conectividad en el frente
- Admite hasta 8 GPU de ancho simple (SW) o 3 de ancho doble (DW) para acelerar cargas de trabajo gráficas intensivas

y rendimiento optimizado para cargas de trabajo para impulsar su negocio.

Características

Experiencia operativa intuitiva en la nube: simple, de autoservicio y automatizada

Los servidores HPE ProLiant DL380 Gen11 están diseñados para su mundo híbrido. Los servidores HPE ProLiant DL380 Gen11 simplifican la forma en que controla la computación de su empresa, desde el límite hasta la nube, con una experiencia operativa en la nube.

Transforme las operaciones comerciales y haga que su equipo pase de reaccionar a proactuar con visibilidad y conocimientos globales a través de una consola de autoservicio.

Automatice las tareas para lograr eficiencia en la implementación, estabilidad instantánea y acceso simplificado y administración del ciclo de vida, reduciendo los errores y acortando los períodos de mantenimiento.

Estas experiencias están diseñadas e integradas en todos los servidores HPE ProLiant Gen11, para que de cómputo con servidores físicos o de contenedores como servicio, elija de HPE GreenLake la mejor manera que satisfaga sus demandas de computación y almacenamiento.

Simplifique y proteja la gestión de servidores desde el borde hasta la nube con HPE GreenLake para Compute Ops Management. HPE GreenLake para Compute Ops Management es una experiencia de gestión informática como servicio que ofrece mayor simplicidad, agilidad y velocidad en todo su parque de servidores físicos, a nivel mundial.

Seguridad confiable por diseño: intransigente, fundamental y protegida

El servidor HPE ProLiant DL380 Gen11 utiliza HPE Silicon Root of Trust, el enfoque fundamental de seguridad de HPE que proporciona una arquitectura de confianza cero a nivel de silicio y garantiza que todo el firmware esencial del servidor esté libre de malware o código comprometido.

El servidor impulsado por procesadores escalables Intel® Xeon® de cuarta generación agrega características de seguridad basadas en hardware y software, incluidas Intel® Software Guard Extensions e Intel® Boot Guard, que aseguran la base del hardware del servidor donde las cuentas aplicaciones críticas se ejecutan y ayudan a proteger los datos en la memoria.

Los servidores HPE ProLiant Gen11 protegen continuamente los servidores en buen estado al proporcionar una detección rápida de servidores con seguridad comprometida, incluso hasta el punto de recuperación, aislar, identificar y contener código malicioso y protege los servidores en el borde con cumplido. Todo esto ocurre de forma predeterminada.

Los servidores HPE ProLiant brindan recuperación automatizada de nivel de seguridad. Incluida la restauración del firmware validado y facilitan la recuperación del sistema operativo, las aplicaciones y los componentes de datos, proporcionando la ruta más rápida para que un servidor vuelva a estar en línea y a sus operaciones normales.

Del silicio al software, de la fábrica a la nube y de generación en generación, HPE ProLiant Gen11 está diseñado con un enfoque de seguridad fundamental para defenderse contra amenazas cada vez más complejas a través de un compromiso inquebrantable con los constantes avances de seguridad que están integrados en nuestro ADN.

Rendimiento optimizado para las cargas de trabajo acelerado, ágiles y eficientes

El servidor HPE ProLiant DL380 Gen11 es un excelente aporte para cargas de trabajo estándar de computación y almacenamiento de dos [illegible] que requieren un número máximo de núcleos, capacidad de GPU y ancho de banda de memoria.

Aproveche el mayor rendimiento de su computadora. El servidor HPE ProLiant DL380 Gen11 cuenta con procesadores escalables Intel® Xeon® de cuarta generación con hasta 60 núcleos por procesador, 350 W y hasta 8 TB de memoria.

El servidor HPE ProLiant DL380 Gen11 proporciona velocidades de transferencia de datos [illegible]

CONSORCIO EMDOC
EMDOC
Santo Domingo, R.D.

320

y mayores velocidades de red desde el bus de expansión serie PCIe Gen5, con hasta 2 x16 ó Cle Gen5 y 2 ranuras OCP para mejorar el rendimiento de E/S y reducir la latencia.

Proporciona 16 canales DIMM por procesador para hasta 8 TB de memoria DDR5 en total con mayor ancho de banda de almacenamiento y rendimiento, y menores requisitos de energía

Proporciona integración con OpenVMS para mejorar el rendimiento del servidor, además de recomendaciones para ajustar la configuración del BIOS y ampliar la vida útil de las unidades empresariales cambiables.

Disponible en una experiencia como servicio

El servidor HPE ProLiant DL380 Gen11 cuenta con el respaldo de HPE GreenLake para simplificar la gestión de la infraestructura de TI en todo su entorno híbrido. Con monitoreo y administración 24 horas al día, 7 días a la semana, nuestros expertos hacen el trabajo pesado para administrar soluciones con servicios integrados en soluciones basadas en el consumo.

Hewlett Packard Enterprise ofrece a los clientes opciones sobre cómo adquirir y consumir TI más allá del financiamiento y el arrendamiento tradicionales, proveyendo opciones que liberan capital estratégico, aceleran las actualizaciones de infraestructura y brindan consumo de pago por uso, todo con HPE GreenLake.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

Especificaciones técnicas — HPE ProLiant DL380 Gen11

Tipo de procesador	Intel®
Familia de procesadores	Procesadores Intel® Xeon® Scalable de 4ª generación y procesadores Intel® Xeon® Scalable de 5ª generación
Número de procesador	1 o 2
Núcleos por procesador disponible	De 16 a 60 núcleos, dependiendo del procesador
Caché del procesador	22,5 MB a 112,5 MB L3, según el procesador
Velocidad del procesador	3,1 GHz máximo, dependiendo del procesador
Instrucciones del procesador	Instrucciones mejoradas de Intel® AVX-512 (AVX-512) en cada núcleo de CPU para una aceleración 2 veces mayor de las cargas de trabajo de HPC, análisis y criptografía
Ranuras de expansión	Hasta 8 PCIe Gen5 y 2 OCP 3.0 para obtener descripciones detalladas, consulte la QuickSpecs
Memoria máxima	8 TB con 256 GB LRDIMM
Ranuras de memoria	32
Tipo de memoria	Memoria inteligente HPE DDR5
Funciones de protección de memoria	ADDC avanzado, repuesto en bajas, duplicación, funcionalidad idéntica con el combinado (bloqueo) y HPE Fast Fault Tolerant Memory (ADDC DC) Memoria persistente Intel Optane
Ranuras unidad óptica	DVD RW opcional (se debe adquirir con la Universal Media Bay 8 SFF) (soporte externo)
Controladora de almacenamiento interno	Hasta dos controladoras de almacenamiento HPE MR compatibles con RAID, modo HBA y modo de conservación de energía de la unidad
Controladora de red	1 GbE, 10 GbE, 10/25 GbE, 100 GbE o 200 GbE, un adaptador PCIe o Flexible OCP 3.0 para obtener descripciones detalladas, consulte las QuickSpecs
Controladoras de almacenamiento	HPE SR932p y/o HPE MR216i-p y/o HPE MR216i-o y/o HPE MR216i-a y/o HPE MR416i-p y/o HPE MR416i-o, para obtener descripciones detalladas, consulte las QuickSpecs
Gestión de infraestructura	HPE iLO Standard (con aprovisionamiento de registro [Intelligent Provisioning], HPE OneView Standard (requiere descarga del instalador), HPE iLO Advanced, HPE OneView Advanced (opcional, requiere licencia) y HPE GreenLake Cloud
Garantía	Para la garantía limitada estándar y otras opciones de piezas, mano de obra y años de cobertura de soporte in situ, consulte la declaración de garantía limitada mundial y el soporte técnico disponibles en https://support.hpe.com/hpsc/public/home. Se encuentran disponibles diferentes niveles de servicio y soporte HPE opcional para complementar la garantía del producto. Para obtener más información, visite https://www.hpe.com/support.
Unidad compatible	Hasta 24 SFF SAS/SATA/NVMe o 48 de 24 SFF SAS/SATA/NVMe, soporte configurable. Con hasta nueve SFF opcionales o unidades nuevas SFF opcionales, 24 SFF NVMe operativas, la compatibilidad con NVMe a través de Express Bay limitará la capacidad máxima de 4 unidades según el modelo

CONSORCIO EMDOC
EMDOC CONSTRUCTORA
Santo Domingo, R.D.

322

Para obtener información técnica adicional, modelos disponibles y opciones, consulte las QuickSpecs

Servicios HPE

No importa en qué etapa de su viaje de transformación se encuentre, nuestro portafolio de servicios HPE puede ayudarle a maximizar la experiencia que necesita cuándo, dónde y cómo la necesita. Desde la estrategia y la planificación hasta la implementación, las operaciones en curso y más, nuestros expertos pueden ayudarle a hacer realidad sus entornos digitales.

Servicios de consultoría

Los expertos pueden ayudarle a acelerar su camino hacia la nube híbrida y optimizar sus operaciones.

Servicios gestionados

HPE ejecuta sus operaciones de TI, brindándole un control certificado para que pueda concentrarse en lo

Innovación, servicios operativos

Optimice todo su entorno de TI e impulse la innovación. Administre las tareas operativas de TI diarias mientras libera tiempo y recursos valiosos.

- Servicio HPE Complete Care: un servicio modular diseñado para ayudar a optimizar todo su entorno de TI y lograr resultados de TI y objetivos comerciales acordados. Todo entregado por un equipo asignado de expertos de HPE.
- HPE Tech Care Service: la experiencia de servicio operativo para productos HPE. El servicio brinda acceso a expertos en productos expertos, una experiencia digital impulsada por AI y orientación técnica general para ayudar a reducir el riesgo y buscar formas de hacer las cosas mejor.

Servicios de ciclo de vida

Aborde las necesidades específicas de su proyecto de implementación con nuestros servicios empresariales y globales de proyectos personalizados.

Servicios educativos de HPE

Capacitación y certificación diseñadas para profesionales de TI y negocios en todas las industrias. Cree rutas de aprendizaje para ampliar el dominio de una materia específica. Programe la capacitación de la manera que mejor funcione para su negocio con opciones flexibles de aprendizaje combinado.

La opción de actualización de servicio de retención de medios defectuosos (DMR) se aplica solo a discos y unidades SSD/Flash elegibles reacondicionados por Hewlett Packard Enterprise debido a un mantenimiento. La cobertura integral de seguridad de datos excluyentes (CDMR) le permite conservar todos los componentes de almacenamiento de datos

HPE GreenLake

La plataforma de borde a nube HPE GreenLake es la oferta como servicio líder en el mercado de HPE que lleva la experiencia de la nube a aplicaciones y datos en todas partes (centros de datos, nubes múltiples y bordes) con un modelo operativo unificado, local y completamente gestionado en un modelo de pago por uso.

Si buscas más servicios, como Soluciones de financiación de TI, explóralos aquí

Explore HPE GreenLake

Tome la decisión de compra correcta.

Hable con un especialista

Chat now (sales)

Call now

Buy now

Share now

Get updates

© Copyright 2021 Hewlett Packard Enterprise Development LP. La información contenida en este documento está sujeta a cambios sin previo aviso. Las únicas garantías para los productos y servicios de Hewlett Packard Enterprise están establecidas en las declaraciones de garantía expresa que acompañan a dichos productos y servicios. Nada de lo aquí incluido debe interpretarse como una garantía adicional. Hewlett Packard Enterprise no se responsabiliza de errores técnicos o editoriales ni de omisiones contenidos en este documento.

Intel, Intel Xeon y Intel Optane son marcas comerciales de Intel Corporation o de sus subsidiarias en los Estados Unidos y en otros países. Todas las demás marcas comerciales son propiedad de sus respectivos dueños.

Este documento se imprimió en papel reciclado
RAHB-[illegible]ESLA, mayo de 2021

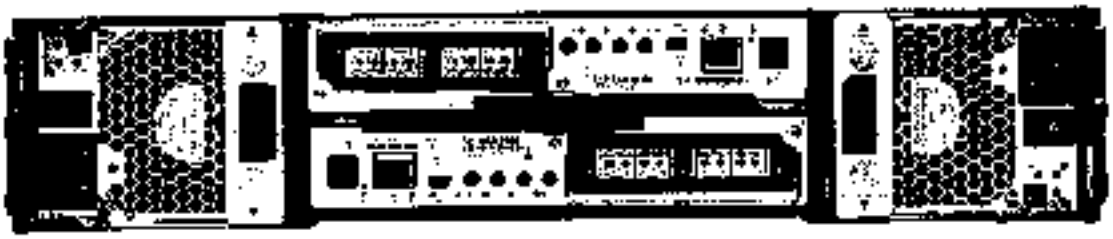
Hewlett Packard Enterprise

CONSORCIO EMDOC
EMDOC
Santo Domingo, RD

Traducido del inglés al español - www.softcoductores.com

HPE GreenLake

Almacenamiento HPE MSA 2062



Qué hay de nuevo

- Dobles de empuje de almacenamiento HPE GreenLake 2062 y opciones de gabinete de unidad HPE MSA 2060 con tarjetas de alimentación con certificación HVAC que cumplen con los requisitos de eficiencia energética ErP Lot 9 2021.
- Amplíe la capacidad de su matriz HPE MSA 2062 agregando un gabinete de unidad 2060 LFF utilizando el nuevo disco duro HPE MSA 20 TB SAS 7.2K LFF. Disponible como opción de unidad única o de paquete de seis.
- Maximice la capacidad de almacenamiento flash de su matriz y unidad HPE MSA 2062 Gabinetes agregando el nuevo SSD HPE MSA 7.68 TB SAS RI SFF.
- Agregue soporte de conectividad de host iSCSI de 25 Gb a su matriz HPE MSA 2062 con el nuevo paquete de 4 transceptores iSCSI de corta alcance HPE MSA 25 Gb SFP28.

Descripción general

¿Busca un almacenamiento flash realmente sencillo y asequible?

El almacenamiento HPE MSA 2062 es un sistema habilitado para flash diseñado para una aceleración de aplicaciones asequible para implementaciones de oficinas pequeñas y remotas. No se deje engañar por el bajo costo. HPE MSA 2062 le ofrece la combinación de simplicidad, flexibilidad y funciones avanzadas que quizás no espere en una matriz de almacenamiento de precio básico. A partir de 3,84 TB de capacidad flash integrada, puede escalar el sistema desde allí con cualquier combinación de discos de estado sólido (SSD), unidades de disco duro SAS empresariales de alto rendimiento o unidades de disco duro SAS midline de menor costo. Capaz de ofrecer hasta 385 000 IOPS, el HPE MSA 2062 le ahorra hasta un 25 % con un paquete de software todo incluido y 3,84 TB de capacidad flash incluidos. Es un almacenamiento flash realmente simple y asequible que lo ayudará a lograr un alto rendimiento y al mismo tiempo cumplir con presupuestos desafiantes.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

- Nuevo disco duro SAS LFF 7.2K de 18 TB de capacidad, unidad única y opciones de paquete de seis disponibles para los modelos de montaje 2062 LFF y gabinetes de unidades de expansión 2060 LFF.

Características

Aceleración de aplicaciones asequible

El almacenamiento HPE MSA 2062 es capaz de ofrecer más de 380 000 IOPS para una aceleración de aplicaciones asequible para pequeñas y medianas empresas

Ahorre un 25 % en HPE MSA 2062 con software todo incluido y 3,84 TB de capacidad de unidad de estado sólido (SSD) incluidos

Los servicios de datos "Configúrelo y olvídese" de HPE MSA no requieren un administrador de almacenamiento dedicado

El almacenamiento HPE MSA 2062 es fácil de instalar, fácil de usar y fácil de mantener, incluso para un generalista de TI. Los administradores encontrarán la nueva utilidad de gestión de almacenamiento de HPE MSA 2062 intuitiva y fácil de navegar.

El nuevo asistente para discos virtuales proporciona a HPE MSA opciones claras para seleccionar los cambios más comunes de RAID para el almacenamiento que hacen que sea fácil y rápido determinar la mejor opción de RAID para sus necesidades.

Aproveche las funciones de protección de datos para mantener su negocio en funcionamiento en caso de desastre

El almacenamiento HPE MSA 2062 ofrece una gama de características avanzadas que hacen que la protección de datos y la recuperación ante desastres sean rentables y sencillas.

La replicación remota asíncrona de Fibre Channel (FC) o iSCSI facilita una solución asequible de recuperación ante desastres

Se pueden implementar SSD y HDD cifrados con administración de claves local para ofrecer una matriz flash híbrida cifrada y segura.

Arquitectura modular y flexible que facilita el crecimiento hacia el futuro

La solución de almacenamiento HPE MSA 2062 admite una combinación de gabinetes de unidades de expansión LFF de 3,5 pulgadas y SFF 2060 de 2,5 pulgadas para un máximo de 12 gabinetes (10 en total, incluida la matriz)

Combine poco a poco y escale según sea necesario con cualquier combinación de SSD Enterprise SAS o Midline SAS HDD.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

Especificaciones técnicas — Almacenamiento HPE MSA 2062

[illegible]	Hasta 12 HDD y/o SSD LFF o 24 SFF por matriz, según el modelo
Capacidad	1.681,72 TB (modelo expansión SFF) a 2.363,84 TB (modelo expansión LFF) por [illegible] según el modelo y la configuración
[illegible]	Canal de fibra de 64 Gb, iSCSI 10/25 GbE, iSCSI 10GBase-T o SAS de 12 Gb según el modelo
[illegible]	2 controladoras por matriz, 4 puertos por controladora para [illegible]
Sistemas operativos compatibles	Servidor Windows 2022 Servidor de Windows 2019 Servidor de Windows 2016 VMWare vSphere 7.0 Red Hat Linux 8 SuSE SUSE 15
[illegible]	2U
Dimensiones del producto (anchura)	8,9x44,5x56,8cm
Peso	[illegible]
Garantía	[illegible]

[illegible]

CONSORCIO EMDOC
EMDOC
Santo Domingo, R.D.

Para obtener información técnica adicional, modelos disponibles y opciones, consulte las QuickSpecs

Servicios HPE

Ya sea que se encuentre en cualquier etapa de su transformación de entorno de trabajo, puede contar con los servicios HPE para brindarle la experiencia que necesita, cuándo, dónde y como la necesita. Desde la estrategia y planificación hasta la implementación, las operaciones en curso y más, nuestros expertos pueden ayudarlo a hacer realidad sus ambiciones digitales.

Servicios de consultoría

Los expertos pueden ayudarlo a recorrer su camino hacia la nube híbrida y optimizar sus operaciones

Servicios operativos

HPE ejecuta sus operaciones de TI brindándole un compromiso basado para que pueda concentrarse en la innovación. Servicios operativos

Optimice todo su entorno de TI e impulse la innovación. Administre las cargas operativas de TI diarias mientras libera tiempo y recursos valiosos.

- Servicios HPE Complete: Es un servicio modular diseñado para ayudarle a optimizar todo su entorno de TI y lograr resultados de TI y objetivos comerciales acordados. Todo entregado por un equipo designado de expertos de HPE.
- HPE TechCare Service: la experiencia de servicio operativo para productos HPE. El servicio brinda acceso a expertos en productos conectados, una experiencia digital impulsada por IA y orientación técnica general para ayudar a reducir el riesgo y buscar formas de hacer las cosas mejor.

Servicios de calidad vida

Aborde las necesidades específicas de su objetivo de implementación con nuestra cartera de soluciones y gestión de proyectos para cualquier nube

Servicios educativos de HPE

Capacitación y certificación diseñadas para profesionales de TI y negocios en todas las industrias. Cree rutas de aprendizaje para ampliar el dominio de una materia específica. Programe la capacitación de la manera que mejor funcione para su negocio con opciones flexibles de aprendizaje continuo.

La opción de retención de medios defectuosos (DMR) se aplica a discos o unidades SSD/Flash elegibles reemplazados por Hewlett Packard Enterprise debido a un mal funcionamiento. La retención integral de medios defectuosos (CDMR) le permite conservar todos los componentes de retención de datos.

HPE GreenLake

La plataforma de borde a nube HPE GreenLake es la oferta como servicio líder en el mercado de HPE que ofrece la experiencia de la nube a aplicaciones y datos en todos los puntos críticos de datos, entre múltiples y bordes: con un modelo operativo unificado, total y con pago por uso.

Si buscas más servicios, como Soluciones de financiación de TI, explóralos aquí.

Explore la colección de ofertas como servicio disponibles en todo el mundo

Ver ofertas como servicio

Chat now (sales)

Call now

Buy now

Share now

Get updates

Hewlett Packard Enterprise

© Copyright 2021 Hewlett Packard Enterprise Development LP. La información contenida en este documento está sujeta a cambios sin previo aviso. Las únicas garantías para los productos y servicios de Hewlett Packard Enterprise son las establecidas en las declaraciones de garantía expresa que acompañan a dichos productos y servicios. Nada de lo aquí incluido debe interpretarse como garantía adicional. Hewlett Packard Enterprise no se responsabiliza por errores técnicos o de edición ni por omisiones contenidas en el presente documento.

Microsoft y Windows son marcas comerciales registradas o marcas comerciales de Microsoft Corporation en los Estados Unidos y/o en otros países.

Linux es una marca comercial registrada de Linus Torvalds en los Estados Unidos y en otros países.

Publicado por Hewlett Packard Enterprise Development LP
[illegible] mayo de 2021

CONSORCIO EMDOC
EMDOC
Santo Domingo, R.D.

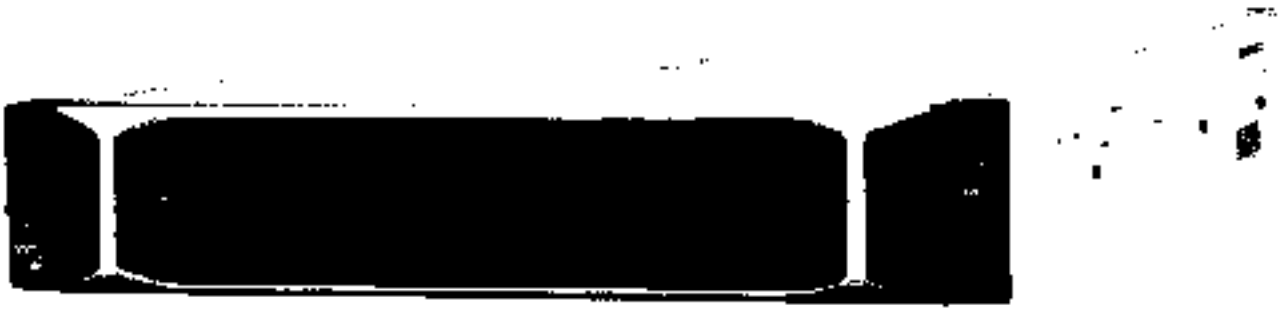
CDS Translation del original español - www.emdocumentos.com

Ficha de datos

HPE GreenLake

Sistemas HPE StoreOnce

1013350029 (R6U02A)



CONSORCIO EMDOC
EMDOC
CONSULTING
Santo Domingo, R.D.

Para obtener información sobre los sistemas y soluciones disponibles, consulte las especificaciones rápidas.

Servicios HPE

No importa en qué etapa de su proceso de transformación se encuentre, puede contar con los servicios de HPE para obtener la experiencia que necesita, cuando, donde y como la necesita. Desde la estrategia y la planificación hasta la implementación, las operaciones en curso y más allá, nuestros expertos pueden ayudarle a hacer realidad sus ambiciones digitales.

Servicios de consultoría

Los expertos pueden ayudarle a iniciar su camino hacia la nube híbrida y optimizar sus operaciones.

Servicios gestionados

HPE asume todas las operaciones de TI, brindándole un control unificado para que pueda concentrarse en la innovación.

Servicios operativos

Optimice todo su entorno de TI e impulse la innovación. Gestione las cargas operativas de TI diarias y, al mismo tiempo, libere tiempo y recursos valiosos.

- Servicio HPE Complete Care: un servicio modular diseñado para ayudar a optimizar todo su entorno de TI y lograr las actitudes de TI y los objetivos comerciales asociados. Todo brindado por un equipo asignado de expertos de HPE.
- Servicio HPE Tech Care: la experiencia de servicio operativo para productos HPE. El servicio brinda acceso a expertos específicos de cada producto, una experiencia digital impulsada por IA y orientación HPE en general para ayudar a reducir el riesgo y buscar formas de hacer las cosas mejor.

Servicios del ciclo de vida

Aborde actividades específicas de proyectos de implementación de TI con servicios de implementación y gestión de proyectos personalizados.

Servicios empleados de HPE

Capacitación y certificación diseñadas para profesionales de TI y negocios de todas las industrias. Cree rutas de aprendizaje para ampliar su competencia en un tema específico. Programe la capacitación de la manera que mejor se adapte a su negocio con opciones flexibles de aprendizaje conjunto.

La opción de servicio de retención de medios defectuosos (DMR) se aplica únicamente a discos o unidades SSD/flash elegibles que Hewlett Packard Enterprise reemplazó debido a un mal funcionamiento. La retención integral de material defectuoso (CDMR) le permite conservar todos los componentes de almacenamiento de datos.

HPE GreenLake

La plataforma de borde a nube HPE GreenLake es la oferta como servicio líder en el mercado de HPE que ofrece la experiencia de la nube a aplicaciones y datos en todos los entornos, lo que acelera la innovación digital, la transformación y la toma de decisiones basada en datos. Con un modelo operativo unificado, todos los resultados, completamente automatizados en un modelo de pago por uso.

Si buscas más servicios, como Soluciones de financiación de TI, por favor explóralos aquí.

Transcribe cualquier dato comercial.

Chat now (sales)

Buy now

Share now

Get updates

Hewlett Packard Enterprise

© Copyright 2021 Hewlett Packard Enterprise Development LP. La información contenida en este documento está sujeta a cambios sin previo aviso. Las únicas garantías de los productos y servicios de Hewlett Packard Enterprise se establecen en las declaraciones de garantía expresa que acompañan a dichos productos y servicios. Nada de lo aquí contenido debe interpretarse como una garantía adicional. Hewlett Packard Enterprise no se responsabiliza de errores técnicos o editoriales ni de omisiones contenidos en este documento.

Pivot3 y marcas HPE, todos los nombres y logotipos de productos de Pivot3 son propiedad de Pivot3 y/o sus filiales en los Estados Unidos y/o en otros países. Todas las demás marcas comerciales son propiedad de sus respectivos propietarios.

Un plazo proporcionado de Hewlett Packard Enterprise para el producto físico o servicio de nube que se describe en la documentación del producto o servicio de Hewlett Packard Enterprise aplicable. El cliente no tendrá derecho a la garantía limitada de Hewlett Packard Enterprise y podrá tener derecho a otros derechos legales según el contrato de compra aplicable u otros acuerdos celebrados entre Hewlett Packard Enterprise y el cliente.

Las imágenes pueden diferir del producto real.
a4_ficha_datos_es_la_es_latam_es_mx_es_co_es_ve_es_ar_es_cl_es_pe_es_ec_es_uy_es_bo_es_py_es_cr_es_pa_es_gt_es_sv_es_hn_es_ni_es_do_es_pr_es_cu

Traducido del inglés al español - www.onlinedoctranslator.com

Hewlett Packard Enterprise

HPE ProLiant Gen11 Gestión de servidores con iLO 6

H37ZSS

Este curso enseña al alumno cómo configurar, actualizar y supervisar un servidor HPE ProLiant Gen11 utilizando productos de administración integrados HPE ProLiant Gen11.

[illegible]	H37ZSS
Duración del curso	2 días
Formato	ILT, VILT
Ver horario, local precios y registro	Ver ahora
Ver cursos relacionados	Ver ahora

5 razones para elegir a HPE como su socio de formación

1. Aprenda de HPE para tecnología de la industria de TI [illegible]
2. Obtenga [illegible]
3. Obtenga un conjunto de habilidades personalizado para [illegible]
4. Logre [illegible]
5. Aprenda [illegible]

Explore [illegible]

Audiencia

Administradores, ingenieros y consultores que configurarán y mantendrán servidores HPE ProLiant Gen11

Prerrequisitos

Los estudiantes deben tener un conocimiento básico de al menos uno de los siguientes sistemas operativos:

- Microsoft Windows Server® 2022
- Servidor empresarial SUSE Linux 15
- VMware® ESXi™ 8.x

Objetivos del curso

Después de completar este curso, usted debería poder

- Diferenciar entre los servidores HPE ProLiant en términos de opciones compatibles, factor de forma y carga de trabajo esperada
- Diferenciarse por propósito productos de gestión integrados de HPE, incluido el procesador de gestión Lights-Out (iLO) integrado, ROM UEFI para ProLiant, [illegible]
- Configurar iLO y la red con las utilidades del sistema UEFI
- [illegible]
- Configurar ajustes de seguridad, ver el rendimiento, umbrales para monitorear la temperatura y la energía
- Diferenciar entre las configuraciones de seguridad en iLO y su impacto en el rendimiento
- Referenciar entre los métodos para monitorear el servidor utilizando la interfaz basada en navegador de iLO y los comandos REST de iLO, así como las aplicaciones basadas en la nube.
- Identificar las etapas y los métodos para actualizar el firmware del servidor.
- Realizar la actualización del firmware del servidor mediante Service Pack para ProLiant (SPP) y Smart Update Manager (SUM)
- Localizar información de diagnóstico de las utilidades del sistema iLO y UEFI
- Diferenciar entre la gestión de iLO y OpenBMC
- [illegible]
- Busque recursos para [illegible] sobre la administración [illegible] ProLiant Gen11 y el [illegible] del servidor

CONSORCIO EMDOC
EMDOC
Santo Domingo, R.D.

Esquema detallado del curso

Módulo 1 Descripción general del hardware y la tecnología HPE ProLiant Gen11	• Descripción general de la familia de servidores HPE ProLiant Gen11 • Seguridad del servidor • Opciones de hardware	• Opciones de software • Opciones de garantía y soporte • Comprobación y conclusiones del apartado del módulo
Módulo 2 Descripción general de los productos de gestión integrados	• Descripción general de los productos de gestión integrada • iLOnet UEFI para HPE ProLiant Gen11 • UIT 6 • Mantenimiento inteligente • Sistema de Salud Activo	• Service Pack para ProLiant y Smart Update Manager • Gestión de operaciones basada en la nube • Controladora de gestión de placa base (BMC) • Comprobación y conclusiones del apartado del módulo
Módulo 3 Configuración del servidor	• Antes de empezar: qué tener en cuenta • Configurar el hardware • Versión de configuración del servidor • Configuración UEFI	• Configuración rápida y mantenimiento del hardware • Configuración del sistema operativo • Comprobación y conclusiones del apartado del módulo
Módulo 4 RBSU	• Introducción a RBSU • Opciones para el acceso remoto • Tareas administrativas • Configuración segura	• Opciones de energía y térmicas • Mantenimiento inteligente y Sistema Activo • Comprobación y conclusiones del apartado del módulo
Módulo 5 Actualización del servidor	• Componentes del sistema • Componentes de E/S	• Controladoras • Comprobación y conclusiones del apartado del módulo
Módulo 6 Mantenimiento del servidor	• Mantenimiento del estado del sistema y de RBSU • Mantenimiento de seguridad y temperatura • Verificación del hardware • Configuración de iLO	• Mejoras del estado del sistema (IEH, UEFI) • Herramientas de prueba (BCM, Advisor) • Comprobaciones y conclusiones del apartado del módulo
Módulo 7 Diagnóstico	• Página de iLO 6 para diagnóstico • Diagnóstico integrado UEFI • Opciones para descargar el registro de AHS	• Indicadores LED del servidor • Comprobaciones y conclusiones del apartado del módulo
Resumen del módulo 8	• Centro de soporte de HPE • Panel de control de Mi centro de software • Cómo acceder al Servicio Education ProLiant	• Evaluación del curso • Resumen del curso y próximos pasos

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

Esquema detallado del laboratorio

[redacted]

Laboratorio 1: Acceso a switches

Laboratorio 2: Acceso a la CLI IOS para switches

[redacted]

Laboratorio 3: Configuración básica de switches

[redacted]

Laboratorio 4: Configuración de switches para aplicaciones de voz

[redacted]

Laboratorio 5: Configuración de switches para aplicaciones de seguridad

[redacted]

Laboratorio 6: Configuración de switches para aplicaciones de alta disponibilidad

[redacted]

Laboratorio 7: Configuración de switches para aplicaciones de calidad de servicio

[redacted]

Laboratorio 8: Configuración de switches para aplicaciones de multicast

[redacted]

Obtenga más información en

http://hpe.com/ww/learnmoreilant

Síganos:

© Copyright 2012 Hewlett-Packard Development Company, L.P. La información contenida en este documento está sujeta a cambios sin previo aviso. Las únicas garantías de los productos y servicios de Hewlett-Packard están establecidas en las declaraciones expresas de garantía que acompañan a dichos productos y servicios. Nada de lo aquí contenido debe interpretarse como una garantía adicional. Hewlett-Packard Enterprise no será responsable de errores u omisiones técnicos o editoriales aquí contenidos.

Todos los demás nombres de marcas son propiedad de sus respectivos dueños.

INT255A-01 agosto de 2012

Hewlett Packard Enterprise

CONSORCIO EMDOC

Traducido del inglés al español - www.onlinedoctranslator.com

HPE aruba networking

Redes HPE Aruba

Serie de interruptores CX 6300



para Edge como:

- Conmutadores apilables de Capa 3 con EGP, EVPN, VXLAN, VRF y OSPF con seguridad y QoS sólidas

- Alto rendimiento con capacidad de conmutación de hasta 1760 Gbps, hasta 1310 MPPS de rendimiento y ancho de banda de apilamiento de hasta 400 Gbps

- Conmutadores compatibles de IL con HPE Smart Rate de (multi-gigabit Ethernet) multigigabit, hasta 90 W PoE (Clase 8) y 10 SR/LRM SFP+ disponibles en modelos seleccionados

Los conmutadores 6300 ofrecen una combinación de hardware, software y herramientas de análisis y automatización de última generación, los conmutadores apilables 6300 forman parte de la cartera de conmutadores HPE Aruba Networking CX, diseñados para las redes empresariales actuales de campus, sucursales y centros de datos

Descripción del producto

La serie de conmutadores HPE Aruba Networking CX 6300 es una familia moderna, flexible e inteligente de conmutadores apilables, ideal para implementaciones de acceso a redes empresariales, agregación, núcleo y centros de datos en la parte superior del bastidor (ToR). Creados para lograr una eficiencia operativa revolucionaria con seguridad y resiliencia integradas, los conmutadores 6300 proporcionan la base para redes de alto rendimiento que admiten aplicaciones de IoT, móviles y en la nube.

Construidos desde cero con una combinación de hardware, software y herramientas de análisis y automatización de última generación, los conmutadores apilables 6300 forman parte de la cartera de conmutadores HPE Aruba Networking CX, diseñados para las redes empresariales actuales de campus, sucursales y centros de datos.

Al combinar un sistema operativo moderno y totalmente programable con el motor de análisis de red HPE Aruba Networking, los conmutadores 6300 brindan capacidades de mantenga y solución de problemas líderes en la industria para la capa de acceso.

Una potente arquitectura ASIC HPE Aruba Networking Gen7 ofrece rendimiento y soporte de funciones sólidos con programabilidad flexible para las aplicaciones del mañana. El marco de apilamiento virtual (VSF) de HPE Aruba Networking permite apilar hasta 10 conmutadores, lo que proporciona estabilidad y gestión simplificada. Cada serie flexible tiene una velocidad de cable incorporada de 1/1 G/2.5/5/10 GbE y enlaces ascendentes de 40/100 GbE y admite PoE de alta potencia IEEE 802.3bt de dos familias. HPE Smart Rate multi-gigabit Ethernet alinea al cliente para puntos de acceso de alta velocidad y dispositivos IoT al ofrecer conectividad rápida sobre alta potencia utilizando cableado estándar

CONSORCIO EMDOC
EMDOC CONSORCIO
Santo Domingo, RD

HPE GreenLake

Características clave y ventajas

- Conjunto de conmutadores de acceso HPE Aruba Networking CX 6300 con hasta 48 puertos de cobre de 1/2.5/5GBASE-T multigigabit y opciones de enlace ascendente de 10/25GbE
- Tres conmutadores de acceso de capa 2, apilables y de alta rendimiento (incremento, clase Aruba HPE Smart Rate Multi-GigaBit y MACsec
- Compatibilidad con redes convergentes de voz, video y datos
- Conectividad de fuji-GbE con QSFP a SFP56 DAC y DAC 50Gb
- Monitoreo, visibilidad y corrección inteligentes con HPE Aruba Networking NetworkAnalytics Engine
- Administre a través de un único panel con HPE Aruba Networking Central a través de cable, inalámbrico y WAN
- Compatibilidad con el software HPE Aruba Networking Switch Identity para configuración y verificación automatizadas
- La segmentación dinámica de HPE Aruba Networking permite un acceso seguro y sencillo para los usuarios y el IoT

Los modelos modulares ofrecen rendimiento alto y flexibilidad de IoT convergentes y compras escalonadas en relación. Rejilla de aire de escape estándar. Suministro de repuesto para implementaciones de centros de datos con pasillo frío caliente (TOR) y administración fuera de banda (OOBM).

La segmentación dinámica extiende la especificidad de políticas establecidas basadas en roles fundamentales de HPE Aruba Networking a los conmutadores cableados de HPE Aruba Networking. Esto significa que se puede disfrutar de la misma seguridad, experiencia de usuario y gestión de TI simplificada en toda la red. Independientemente de cómo se segmentan los usuarios y los dispositivos de IoT, las mismas políticas coherentes en las redes cableadas e inalámbricas, manteniendo el tráfico seguro y separado.

Diferenciadores de producto

Aruba OS-CX, un sistema operativo moderno, se basa en los conmutadores HPE Aruba Networking CX 6300 de base. AOS-CX, un sistema operativo moderno, basado en bases de datos que supropodya y simplifica muchas tareas de red críticas y complejas. Una base de datos de series temporales incorporada permite a los clientes y desarrolladores crear secuencias de comandos de software para la resolución de problemas históricos, las tareas de análisis de condiciones pasadas, ESO ayuda a prever y evitar problemas futuros debido a cualquier tipo de evento de seguridad y rendimiento. Además, el AOS-CX está construido sobre una arquitectura modular de linux con una base de datos compartida, aumentando la eficiencia operativa y proporciona las siguientes capacidades únicas:

- El flujo de trabajo a todo el información del estado de la red permite una visibilidad y análisis únicos
- API REST y secuencias de comandos Python para una programabilidad simplificada de tareas de red
- Una arquitectura de microservicios que permite la integración total con dispositivos de hardware.

Sistemas y servicios

- Datos de telemetría continuos con capacidades analíticas integradas para aumentar la importancia por eventos
- Sincronización de estado continua que proporciona una tolerancia superior a fallas y alta disponibilidad

- Todos los procesos de software se comunican con la base de datos en lugar de enviar un paquete, lo que garantiza un estado y estándar común. Simplificación y permite que los módulos de software individuales se actualicen de forma independiente para una mayor disponibilidad.

Cada conmutador CX incluye AOS-CX sin costo y con un conjunto sólido y completo de características software que le permiten implementar, corregir y solucionar problemas de una red inteligente, que incluye:

- Motor de análisis de red (NAE)
- Segmentación dinámica
- Alta disponibilidad y resiliencia
- Calidad de servicio (QoS)
- Conmutación de capa 2
- Servicios y enrutamiento de capa 3
- Multidifusión IP
- Seguridad de la red
- Compatibilidad con el software de código abierto del mismo proveedor de red HPE Aruba

Además de las funciones estándar disponibles en AOS-CX, ofrecemos un paquete de funciones mejoradas HPE Aruba Networking CX opcional y basado en términos que desbloquea la versatilidad y flexibilidad de la seguridad avanzada.

Para obtener más información, lea la Guía de pedido de paquete de características de HPE Aruba Networking CX

HPE Aruba Networking Central: gestión unificada de panel único

HPE Aruba Networking Central es una solución inteligente por la que simplifica las operaciones de TI, mejora la agilidad y reduce los costos al unificar la gestión de toda la infraestructura de red. Diseñado para brindar resiliencia y seguridad de nivel empresarial, aunque es lo suficientemente simple para una mediana empresa con personal de TI limitado. HPE Aruba Networking Central es la consola única de visibilidad y control que abarca toda la red, desde la sucursal hasta el centro de datos, desde la LAN cableada e inalámbrica hasta la WAN.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

Disponible como una solución local o basada en la nube, HPE Aruba Networking Central se diseñó para simplificar las operaciones del día 0 al día 2 con flujos de trabajo optimizados para la creación de sitios, la creación de plantillas de configuración basadas en IA y NAE así como con una vista unificada de todos los dispositivos y usuarios, tanto cableados como inalámbricos. Las capacidades integrales de administración de conmutadores incluyen configuración, incorporación, monitoreo, resolución de problemas e informes.

Una suscripción a HPE Aruba Networking Central Foundation NE permite capacidades integrales de administración de conmutadores que incluyen configuración, incorporación, monitoreo, resolución de problemas e informes. Una suscripción a HPE Aruba Networking Central Advanced amplía estas capacidades con seguridad premium y AIOps, incluido HPE Aruba Networking Central NetConductor Fabric Wizard y Policy Manager para permitir la segmentación dinámica y la aplicación distribuida a escala global.

Además, una suscripción a HPE Aruba Networking Central Advanced habilita el CX Advanced Feature Pack, por lo que no es necesario comprar por separado un CX Advanced Feature Pack. Esto optimiza la eficiencia operativa y reduce la necesidad de que su equipo de TI realice un seguimiento de múltiples suscripciones, términos activos y fechas de renovación.

Para obtener más información sobre las suscripciones a HPE Aruba Networking Central, consulte la Guía de pedidos de suscripciones a HPE Aruba Networking Central SaaS.

Motor de análisis de red HPE Aruba Networking: supervisión y diagnóstico avanzados

Para mejorar la usabilidad y la resolución de problemas, el motor de análisis de red (NAE) de HPE Aruba Networking monitorea y emite alertas automáticamente los eventos que pueden afectar el estado de la red.

La alternancia y la autocorrección avanzadas brindan la capacidad de identificar y solucionar fácilmente problemas relacionados con la red, el sistema, las aplicaciones y la seguridad a través de el uso de agentes Python, agentes basados en CLI, agentes basados en CLI y API REST.

La base de datos de series temporales (TSDB) almacena datos de configuración y estado operativo, lo que los pone a disposición para resolver rápidamente los problemas de red. Los datos también se pueden utilizar para analizar tendencias, identificar anomalías y predecir requisitos de capacidad futura.

HPE Aruba Networking Central utiliza NAE y agentes para ofrecer monitoreo de conmutadores, análisis y solución de problemas mejorada para la seguridad del cableado. El software HPE Aruba Networking Switch Multi-Edit y las herramientas de terceros, como ServiceNow y Slack, brindan la inteligencia para integrar alertas NAE en los procesos de gestión de servicios de TI, acelerando la resolución de problemas.

Software de edición múltiple del conmutador de red HPE Aruba: configuración y gestión automatizadas del conmutador

El sistema HPE Aruba Networking CX permite a los equipos de TI integrar variables de configuración de conmutadores para implementar los protocolos de servicios de red más a menudo. El software HPE Aruba Networking Switch Multi-Edit proporciona automatización que permite cambios rápidos en todo la red y garantiza el cumplimiento de las políticas después de las actualizaciones de la red. Las capacidades integrales incluyen funciones de búsqueda, edición, validación previa a la verificación de conformidad, implementación y auditoría. Las capacidades incluyen:

- Configuración contextual con validación de coherencia y cumplimiento.
- Ahorro de tiempo gracias a la visualización y edición simultáneas de múltiples configuraciones.
- Ingesta de variables personalizadas para cumplimiento, conformidad y planes de cambios de red.
- Implementación automatizada de configuración a gran escala sin programación.
- Visibilidad del estado de la red y de la topología a través de la integración NAE de HPE Aruba Networking.

Nota: se requiere una licencia de software independiente para utilizar el software de edición múltiple del conmutador de red HPE Aruba.

Aplicación móvil HPE Aruba Networking CX: verdadera comodidad de mantenimiento

Una aplicación móvil fácil de usar simplifica la conexión y administración de conmutadores HPE Aruba Networking CX 6300 para proyectos de cualquier tamaño. La información del conmutador también se puede importar al software de edición múltiple del conmutador de red HPE Aruba para simplificar la gestión de la configuración y validar continuamente la conformidad de las configuraciones en cualquier lugar de la red. La aplicación móvil HPE Aruba Networking CX está disponible para descargar.

Innovación programable: HPE Aruba Networking ASIC basados en más de 30 años de invención ininterrumpida, los ASIC de HPE Aruba Networking crean la base para avances de funciones de software ágiles e innovadores, un rendimiento incomparable y una visibilidad profunda. Estos ASIC programables están diseñados específicamente para permitir una integración más estrecha del hardware y software del switch dentro de las arquitecturas de campus y centros de datos para optimizar el rendimiento y la capacidad. La cola de salida virtual (VOQ) evita la congestión, evita el bloqueo de cabecera de línea (HOLB) y permite una velocidad de línea completa en los puertos de salida (salida). Los motores ASIC flexibles permiten que la solución VAE de HPE Aruba Networking inspeccione todos los datos, lo que permite capacidades de análisis líderes en la industria. HPE Aruba Networking CX 6300 se basa en la arquitectura ASIC HPE Aruba Networking Gen7.

Segmentación dinámica de redes HPE Aruba: estructura de campus y sucursales

La solución HPE Aruba Networking Dynamic Segmentation permite una movilidad perfecta, una aplicación consistente de políticas y configuraciones automatizadas para clientes cableados e inalámbricos en redes de acceso por cable unificadas. El acceso basado en roles y la aplicación de políticas en redes LAN, WLAN y SD-WAN, con una definición de política centralizada y puntos de aplicación dedicados, lo que garantiza que los usuarios y dispositivos solo puedan comunicarse con destinos consistentes con su función, manteniendo el tráfico seguro y segregado.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

La segmentación dinámica se basa en establecer un acceso con privilegios mínimos a los recursos de TI mediante la segmentación del tráfico según la identidad, un concepto fundamental de los marcos Zero Trust y SASE donde la confianza se basa en roles y políticas, no en ubicación y cómo se conecta un usuario o dispositivo.

Esta innovación combina puertos inteligentes y tecnologías de microsegmentación basadas en roles. Los puertos inteligentes permiten que los clientes cableados se conecten a cualquier puerto del switch con la configuración automatizada mediante control de acceso basado en RADIUS. Esto elimina la necesidad de reconfigurar manualmente dispositivos IoT o la red.

La microsegmentación basada en roles ofrece beneficios de reducción de la expansión de subredes y VLAN, definición de políticas simplificada y aplicación de políticas escalable a medida que crece el conjunto de roles de usuario. Independientemente de las construcciones de red, como VLAN y VRF, los clientes se pueden agrupar en una función de usuario según su identidad, lo que garantiza que la tecnología de puertos inteligentes se extienda más allá de una superposición centralizada, a medida que los clientes se integran con la creación automática de túneles basada en la política de roles de usuario asociados. La política basada en usuarios ofrece la opción de una microsegmentación utilizando políticas de aplicación personalizadas y unificadas para dispositivos inalámbricos y por cable con firewall con estado de Capa 7 en puertas de enlace o un entorno distribuido con una ACL de rol de Capa 4 en conmutadores.

La segmentación dinámica proporciona escalabilidad y flexibilidad en el diseño de la red, ya que permite la extensión de VLAN y subredes en toda la red con una estructura superpuesta distribuida basada en EVPN/VXLAN. Las superposiciones de túnel utilizan túneles VXLAN a VXLAN-GBP en el plano de datos y brindan la opción de un plano de control BGP EVPN multiprotocolo para implementaciones grandes o un plano de control aplicado de Capa 2 para implementaciones simplificadas.

Rendimiento de escalabilidad y IoT

La serie de conmutadores HPE Aruba Networking CX 6300 está pensada para ofrecer un rendimiento constante que cumple los ASIC HPE Aruba Networking Gen7. Esto garantiza que nuestros conmutadores ofrezcan una latencia muy baja y una mayor inmunidad de ráfagas.

Simultáneamente, el túnel + conducto de control adicional toda la comunicación y el aprovisionamiento se autorizan de cero para soluciones de empresas de rápido crecimiento. Un ancho de banda escalable y futuro. Cada miembro proporciona lo siguiente:

- Hasta 1760 Gbps de ancho de banda sin bloqueo y hasta 1310 Mpps para reenvío
- Enlaces ascendentes de 1/10/25/40/50/100Gby tamaños de TCAM granular ideales para implementaciones de movilidad e IoT en campus grandes con conectividad de clientes
- Configuraciones de cola seleccionables que permiten un mayor rendimiento al definir una cantidad de colas y almacenamiento en búfer de memoria asociado para satisfacer mejor los requisitos de las aplicaciones deseadas.

Aprovisionamiento VSF: rápido y simplificado El marco de conmutación virtual (VSF) de HPE Aruba Networking le permite hasta diez conmutadores de red mediante el aprovisionamiento del plano virtual de alto rendimiento. Las características adicionales incluyen:

- Compatibilidad con hasta 10 conmutadores en una topología en cadena con anillo
- Flexibilidad para crear pilas que abarquen distancias más largas, como cientos de metros o miles de campus haciendo más con menos enlaces, utilizando transceptores de 10 GbE/25 GbE de largo alcance
- Pila básica para conmutadores modulares HPE Aruba Networking 6300 y fijos en una sola pila para satisfacer sus necesidades, requisitos de implementación.
- Configuración y gestión simplificadas ya que los conmutadores actúan como un único cuando se unen
- Alta disponibilidad por diseño durante las actualizaciones. Incluso el soporte ISSU con actualizaciones VSF Rolling Stack (requiere 4 miembros en pila VSF de 2 miembros)
- La solución virtual HPE Aruba Networking Orchestrator solo está disponible para implementaciones de campus que incluyen switches de pila y no pilas, y no admite implementaciones de campus distribuidos.

Un conmutador HPE Aruba Networking CX 6300 para cualquier entorno empresarial Ya sea en una sucursal o en un entorno empresarial pequeño o grande, puede elegir entre modelos 1 de 24 y 48 puertos. Cada conmutador incluye cuatro enlaces ascendentes integrados de alta velocidad que pueden aprovisionarse como 1 GbE, 10 GbE, 25 GbE, 40 GbE y 100 GbE para ofrecer un rendimiento sin bloqueo. Los modelos de formato flip (F) incluyen fuentes de alimentación integradas. Los modelos modulares (M) definen futuros límites para adaptarse a módulos intercambiables en caliente que le permiten personalizar sus requisitos de PoE, y sus ventiladores son reemplazables en campo, aspectos destacados adicionales:

- Los modelos con hasta 48 admiten:
  - 24 y 48 puertos de HPE Smart Rate Multi-gigabit Ethernet IEEE 802.3bz (100M/2.5GbE/5GbE/10GbE) que admiten IEEE 802.3bt con alta potencia Clase 6 (60 W) o Clase 8 (90 W)
  - Modelo SFP+ de 24 puertos de alta densidad que es ideal para agregación
  - Enlace ascendente 1/10/25/40/50/100GbE conectividad de puerto
- HPE Smart Rate Multi-Gigabit (IEEE 802.3bz) Ethernet admite puntos de acceso inalámbricos de alta velocidad
- Para implementaciones que necesitan mayor densidad de puertos y PoE, el 6300 admite hasta 90 W por puerto y un conmutador de 48 puertos para un total de 2880 W de PoE
- La compatibilidad con PoE de alta potencia (Clase 6) y extensión de la tecnología IEEE 802.3bt proporciona hasta 90 W para admitir todos los dispositivos y AP de IoT. La compatibilidad con PoE para IEEE 802.3at, Power over Ethernet (PoE+) proporciona hasta 30 W por puerto), así como cualquier 60E
  Dispositivo heredado compatible con 802.3af
- La compatibilidad con la detección PoE prevista garantiza proporciona energía a dispositivos PoE heredados
- Alta disponibilidad con PoE empresarial activo que se mantiene en el PoE incluso durante reinicios programados y actualizaciones de firmware

Que no solo garantiza un simple PoE, sino que también proporciona [illegible] para el presupuesto de energía [illegible] que no solo [illegible] sino también [illegible] operativo [illegible]

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

- compatibles con Ethernet 10G de eficiencia energética 802.3az reduce el consumo de energía durante períodos de poco tráfico de red.

- Compatibilidad con supervisión óptica digital de diagnóstico (DOM) en la mayoría de los transceptores SFP+ 10GbE compatibles para proporcionar información de diagnóstico en tiempo real sobre el estado del enlace de fibra óptica

- Auto-MDIX proporciona ajustes automáticos para cables directos o cruzados en todos los puertos 10BASE-T/100BASE-TX y Smart-Rate

- El modo de transceptor Network Interface Unit (NIU) permite encender y habilitar todos los transceptores y cables de 1/10/40/50/100GbE no compatibles. Tenga en cuenta que no hay garantía ni soporte para el funcionamiento cuando se utiliza esta función

- Las capacidades de IPv6 incluyen:

  - El host IPv6 permite el administrador conmutadores en una red IPv6

  - Transiciones de pila dual (IPv4 e IPv6) de IPv4 a IPv6, admitiendo conectividad para diversos protocolos

  - La vigilancia MLD reenvía el tráfico de multidifusión IPv6 a los interfaces adecuados

  - IPv6 ACL/QoS admite ACL y QoS para el tráfico de red IPv6

  - El enrutamiento IPv6 admite protocolos estáticos y OSPFv3

  La seguridad proporciona protección RA, prevención DHCPv6 bloqueo dinámico de IPv6, vigilancia ND, protección de destino IPv6, protección DHCP IPv6 y protección de suplantación de identidad IPv6

Las ranuras para ventiladores redundantes de cambio en caliente y fuentes de alimentación de CA/CC proporcionan un tiempo de funcionamiento de 24/7 horas

- Protección contra formación de paquetes (Storm Prevention) de difusión y multidifusión desconocidas definida por el usuario

- El enlace inteligente permite una redundancia de enlace convergente simple y rápida y la capacidad de migración sobre servidores compatibles con varias tarjetas de red

Conmutadores CX 6300: de capa 2 Hay tres modelos de conmutadores CX 6300: disponibles para clientes que buscan escalabilidad, alta capacidad y versatilidad.
Conectividad multicapa de acceso 1 de velocidad local incluyen.

- 24 puertos SR10 (1G/2.5G/5G/10G) o 48 puertos SR6 (1G/2.5G/5G) Enlaces descendentes HPE SmartRate Multi-Gigabit Ethernet que admiten alta potencia IEEE 802.3bt (Clase 6 (60 W) e Clase 8 (90 W) PoE y MACsec-256

- Escalabilidad con apilamiento del plano frontal de hasta 10 miembros de conmutadores CX 6300F o se apila con conmutadores CX 6300F o CX 6300M

- Conmutación de capa 2 con soporte para enrutamiento estático básico de IPv4/IPv6, listas de control de acceso (ACL) y niveles basados en reglas para seguridad y flexibilidad

Requiere CX 6300M: para versión de datos El puerto de comunicación de administración dedicado CX 6300M de 1G puerto fuera de banda como interfaz de gestión (OOBM) de 1 GbE y también como conmutador de puerto de banda (IBM) de 1 GbE para bordes de servidor de centros de datos tradicionales incluyen

- El paquete de almacenamiento puerto (LSAM) incluye un conmutador de 1 GbE de 48 puertos con 2 unidades de ventilador (JL714) y 1 fuente de alimentación (JL706)

- Agregue una combinación de hasta cuatro módulos de 10 GbE

- 1/10/25/50 GbE en cuatro ranuras compatibles

Alta disponibilidad y resiliencia. Para garantizar un alto grado de tiempo de actividad, dirección alta disponibilidad y funciones de multiplexación inteligente para una implementación completa de Capa 3 en acceso y agregación, como PBR, BFD, MSDP, DSR e IP SLAs o necesidad de licencias de software. Esto incluye:

- Fuentes de alimentación redundantes intercambiables en caliente disponibles en los modelos 6300 "M"

- Proporciona redundancia N+1 y N+N para ventiladores configurados en caso de fallo en la línea eléctrica o en el suministro.

- Fuentes de alimentación secundarias opcionales para aumentar la potencia total disponible

- Ranuras de alimentación fijas en modelos 6300 "F"

- La detección bidireccional (BFD) permite la detección de fallos en menos de un segundo para un rápido restablecimiento del protocolo de enrutamiento y admite redes IPv4 e IPv6

- El Protocolo de redundancia de enrutador virtual (VRRP) permite que grupos de dos enrutadores creen dinámicamente entornos enrutados de alta disponibilidad en redes IPv4 e IPv6.

- Detección de enlace unidireccional (UDLD) para monitorear la conectividad del enlace y cerrar puertos en ambos extremos si se detecta tráfico unidireccional, evitando bucles en redes conmutadas en capa 2

- IEEE 802.3ad LACP admite hasta 256 LAG, cada uno con hasta 8 enlaces por LAG, y proporciona soporte para grupos estáticos o dinámicos y un algoritmo hash seleccionable por el usuario.

- El árbol de expansión múltiple IEEE 802.1 proporciona alta disponibilidad de enlaces en entornos VLAN donde se requieren múltiples árboles de expansión, y soporte heredado para IEEE 802.1D e IEEE 802.1w

- El protocolo de control de agregación de enlaces (LACP) IEEE 802.3ad y mejoras propias de nuestros clientes admiten enlaces troncales estáticos y dinámicos, desde cada troncal admite hasta ocho enlaces agrupados por control central

- Compatibilidad con balanceo con Network Load Balancer (NLB) para aplicaciones de servidor

- La conmutación de protección de anillo Ethernet (ERPS) admite protección y recuperación rápidas en una topología de anillo

- Compatibilidad con tramas gigantes CX 6300 independiente y para 6300 con apilamiento VSF

Funciones de calidad de servicio (QoS) Para respaldar acciones de congestión y priorización del tráfico, HPE Aruba Networking CX 6300 Series incluye lo siguiente:

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

- Cola de prioridad estricta (SP) y round robin ponderado por déficit (DWRR)
- Priorización del campo IEEE 802.1p para clasificación en tiempo real en 8 niveles de prioridad que se asignan a 8 colas
- Priorización de capa 4 basada en números de puerto TCP/UDP
- La Clase de Servicio (CoS) establecida en IEEE Etiqueta de prioridad 802.1p basada en dirección IP, tipo de servicio IP (ToS), protocolo de capa 4, número de puerto TCP/UDP, puerto de origen y DiffServ
- La limitación de velocidad establece límites aplicados de ingreso por fuente y mínimos por persona y por cola
- Las velocidades de transmisión de tramas de salida se pueden limitar por cola utilizando Egress Queue Shaping (EQS)
- Grandes buffers para una gestión elegante de la congestión

Configuración y gestión simplificadas

Además de HPE Aruba Networking Central, la aplicación móvil HPE Aruba Networking Central, el software de edición múltiple del conmutador HPE Aruba Networking y el motor de análisis de red HPE Aruba NetVisor, la serie 6300 ofrece lo siguiente:

- Interfaz API REST integrada, programable y fácil de usar
- Aprovisionamiento sencillo centrado en dispositivos
- Monitoreo y capacidad de redes de velocidad de cable escalables basadas en ASIC sin impacto en el rendimiento de la red. Los operadores de red pueden recopilar una variedad de estadísticas e información de red para fines de planificación de capacidad y monitoreo de red en tiempo real
- Se admite la actualización sin interrupciones de software (ISSU) para cada uno de los siguientes según los protocolos de seguridad, siguiendo la ruta de actualización recomendada:
- CLI estándar de la industria con una estructura jerárquica para reducir el tiempo y los gastos de capacitación. Ofrece mayor productividad en entornos de múltiples proveedores
- La seguridad de administración restringe el acceso a comandos de configuración críticos, proporciona múltiples niveles de privilegios con protección por contraseña y capacidad de registro (localmente y remoto que permite registro con 6 niveles de gravedad)
- SNMP v3 proporciona soporte de captura y lectura SNMP de la base de información de administración (MIB) estándar de la industria y extensiones privadas
- La compatibilidad con sFlow® incluye configuración de velocidad de captura y límite, capacidad de agente de contador, polling de POE de interfaz, administración de configuración de contador, CPU y memoria promedio, otra MIB de SNMP
- La compatibilidad con sFlow® incluye compatibilidad con RFC 3176 sFlow, una asociación SNMP MIB-SNMP, MIB SNMPv3, MIB de puerto secundario de puerto, MIB de configuración, MIB de servidor VRF, capacidad de prioridad AAA
- Monitoreo remoto (RMON) con SNMP estándar para supervisar la red esencial funciones. Admite grupos de eventos, alarmas, historial y estadísticas, así como un grupo de extensión de alarma privada. RMON y sFlow brindan capacidades avanzadas de monitoreo y generación de informes para estadísticas, historial, alertas y eventos.
- La exportación de información de flujo de IPFIX permite la recopilación de información de flujo de otros para mejorar la visibilidad
- Simplifica la configuración de conmutadores con Zero Touch Provisioning mediante el uso de aprovisionamiento del protocolo de puerta de enlace de borde de enlace (BGP) para establecer un grupo de conmutadores semilleros dentro de un rango de IP.
- Proporciona información sobre alarmas, tablas y eventos de error a través de HPE Aruba Networking Central para mejorar la visibilidad durante la incorporación del cliente.
- El soporte TFTP y SFTP ofrece diferentes mecanismos para actualizaciones de configuración. FTP (File) (FTP) permite transferencias bidireccionales a través de una red TCP/IP. El Protocolo seguro de transferencia de archivos (SFTP) se ejecuta a través de un canal SSH para proporcionar seguridad adicional
- La utilidad de depuración y mantenimiento admite ping y traceroute para IPv4 e IPv6
- El protocolo de tiempo de red (NTP) sincroniza el cronometraje entre clientes y servidores de tiempo distribuidos; mantiene el cronometraje constante entre todos los dispositivos dependientes del tiempo dentro de la red para que los dispositivos puedan compartir una base de tiempo consistente para diversas aplicaciones basadas en el tiempo (marcas de tiempo)
- El protocolo de descubrimiento de capa de enlace (LLDP) IEEE 802.1AB anuncia y recibe información de administración de dispositivos, aplicaciones en una red, lo que facilita el mapeo por parte de las aplicaciones de administración de red
- Las [illegible] admiten implementaciones [illegible] que [illegible] para [illegible] seguridad durante la [illegible]
- Admite [illegible] para [illegible] a los puertos para una [illegible]
- Seguridad simultánea [illegible] configuración en una [illegible]
- La supervisión de los puertos de entrada y salida permite una resolución más rápida de otros problemas de red
- La detección de enlace unidireccional (UDLD) monitorea el enlace entre dos conmutadores y bloquea los puertos en ambos extremos del enlace si el enlace se cae en cualquier punto entre los dos dispositivos.
- IP SLA para voz monitorea la calidad del tráfico de voz utilizando UDP Jitter y UDP Jitter para pruebas de VoIP.
- El protocolo de tiempo de precisión (PTP) permite una sincronización precisa del reloj entre conmutadores de red o similares, tal como se define en IEEE 1588. El relay transparente (TCP-TL) y el reloj de límite (PTP-BC) son mecanismos para aplicaciones en las que el tiempo es crítico. Con la sincronización de la energía de la red inteligente, los relojes de límite y de transparencia utilizan el reenvío de mensajes de tiempo de 2 pasos.

Compatibilidad de capa 2

Se admiten los siguientes servicios de capa 2:

- Soporte de VLAN y etiquetado para IEEE 802.1Q (4094 VLAN y 4 VLAN)
- La compatibilidad con pares agrupados mejora el rendimiento de grandes transferencias de [illegible] mientras [illegible] de [illegible]

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

- Las VLAN con protocolo IEEE 802.1v están protocolos seleccionados que no son IPv4 automáticamente en sus propias VLAN

- El árbol de expansión rápido por VLAN (RPVST+) permite que cada VLAN construya un árbol de expansión separado será mejorar el uso del ancho de banda del enlace es compatible con PVST+

- MVRP permite el aprendizaje automático y la asignación dinámica de VLAN

- Protocolo de encapsulación (tunelización) VXLAN para red superpuesta que permite una implementación de red virtual más escalable.

- Túnel de unidad de acceso de protocolo de puente (BPDU): transmite BPDU STP de forma transparente, lo que permite cálculos de árbol correctos entre proveedores de servicios, WAN o MAN

- La duplicación de puertos duplica el tráfico de puerto (entrada y salida) a un puerto de monitoreo, admite 4 grupos de duplicación

- STP admite el estándar IEEE 802.1D STP, el protocolo de árbol de expansión rápida (RSTP, IEEE 802.1w) para una convergencia más rápida y el protocolo de árbol de expansión múltiple (MSTP) IEEE 802.1s.

- Protocolo de administración de grupos de Internet (IGMP snooping): Controla y administra la inundación de paquetes de multidifusión en una red de Capa 2

- La compatibilidad con multidifusión IPv4 en VXLAN EVPN Overlay permite el escalonamiento IGMP en VXLAN Overlay.

- Compatibilidad con superposición IPv6 VXLAN/EVPN, permite el tráfico IPv6 a través de la superposición VXLAN.

- La supresión de VXLAN ARP/ND permite minimizar la inundación de tráfico ARP y ND dentro de segmentos VXLAN individuales, optimizando así la red VXLAN.

- Soporte QinQ para mejorar la utilización de VLAN agregando otra etiqueta 802.1Q a los paquetes encapsulados

Servicios de capa 3

Se admiten los siguientes servicios de capa 3:

- La detección de reenvío bidireccional (BFD) permite monitorear la conectividad del enlace y reducir el tiempo de convergencia de red para rutas estáticas, OSPFv2 y VRRP.

- La función auxiliar del protocolo de datagrama de usuario (UDP) permite que las transmisiones UDP se dirijan a través de las interfaces del enrutador a direcciones IP específicas de unidifusión, transmisión de subred y entre subredes de servidores para paquetes UDP como DHCP

- La dirección de la interfaz de bucle invertido define una dirección en el primer salto de enrutamiento (OSPF), lo que mejora la flexibilidad de diseño de red

- Los mapas de rutas brindan más control durante la redistribución de rutas, permiten filtros y alteran métricas de ruta

- El Protocolo de resolución de direcciones (ARP) determina la dirección MAC de otro host IP en la misma subred; admite ARP estáticas; ARP gratuito permite detección de direcciones IP duplicadas; proxy ARP permite eficientemente un conocimiento de ARP entre subredes o cuando las subredes están separadas por una red de Capa 2

- El Protocolo de configuración dinámica de host (DHCP) simplifica la gestión de grandes redes IP y admite clientes; DHCP Relay permite el funcionamiento de DHCP en subredes.

- El servidor DHCP centraliza y reduce el costo de la gestión de direcciones IPv4

- El Sistema de Nombres de Dominio (DNS) proporciona una base de datos distribuida que traduce nombres de dominio y direcciones IP, lo que simplifica el diseño de la red para clientes y servidores

- Una vez que el host IGMP (Internet Group Management Protocol) se une a un grupo multicast, el host IGMP o la tabla de filtros L2

- La descubierta de vecinos (ND) permite conocer el mismo que un vecino está en el mismo enlace de una red de capa 2.

- Admite pruebas de loopback interno para fines de mantenimiento y mayor disponibilidad; La detección de bucle puede protegerse contra configuraciones de red o cableado incorrectos y se puede habilitar por puerto o por VLAN para mayor flexibilidad.

- La subinterfaz IP es una interfaz virtual creada dividiendo la interfaz física en múltiples interfaces lógicas etiquetadas usando diferentes VLAN-ID. Una interfaz física puede ser una interfaz física normal, un puerto troncal o LAG (L2). Se utiliza una subinterfaz para muchos casos de uso, como la interconexión VRF-lite y el enrutamiento inter-VLAN (enrutador integrado).

Servicios de capa 3

Se admiten los siguientes servicios de enrutamiento de capa 3:

- Border Gateway Protocol (BGP) proporciona enrutamiento IPv4 e IPv6, que es escalable, robusto y flexible

- El Protocolo de puerta de enlace fronteriza 4 (BGP-4) ofrece una implementación del Protocolo de puerta de enlace exterior (EGP) utilizando vectores de ruta sobre TCP para mejorar la confiabilidad del proceso de descubrimiento de rutas; reduce el consumo de ancho de banda al enviar solo actualizaciones incrementales; apoya políticas amplias para una mayor flexibilidad; escala a redes muy grandes con capacidad de reinicio elegante

- Equal Cost Multipath (ECMP) permite múltiples enlaces de igual costo en un entorno de enrutamiento para aumentar la redundancia de enlaces y ofrecer un mayor ancho de banda

- BGP multiprotocolo (MP-BGP) permite compartir rutas IPv6 usando BGP y comunicarse con pares BGP usando IPv6

- El Protocolo de Información de enrutamiento versión 2 (RIPv2) proporciona un protocolo de enrutamiento fácil de configurar para redes pequeñas, ideal en aquellos casos en los que RIPng es una buena opción para redes IPv6 pequeñas

- Abrir primero el camino más corto (OSPF) ofrece una convergencia más rápida; un rápido protocolo de puerta de enlace interior (IGP) de enrutamiento de estado de enlace, que admite autenticación (OSPF, IS-IS, RIPv2, BGP) para una mayor seguridad y enrutamiento jerárquico con una delimitación de límites más clara

- OSPF proporciona OSPFv2 para enrutamiento IPv4 y OSPFv3 para enrutamiento IPv6

- El enrutamiento IP estático proporciona enrutamiento configurado manualmente, lo cual es útil en redes pequeñas

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

- Reenvío/enrutamiento basado en políticas (PBR) de flujos definidos para seleccionar el túnel que se puede usar en la interfaz de salida establecida para el destinatario de la red

- El conmutador IPv4 e IPv6 ofrece proporciones mixtas IPv4 y IPv6 admitidas y configuradas manualmente.

- La optimización del rendimiento IP proporciona un conjunto de herramientas para mejorar el rendimiento de las redes IPv4, incluyendo transmisiones dirigidas, personalización de parámetros TCP, soporte de paquetes de error ICMP y amplias capacidades de visualización

- La pila IP dual mantiene pilas separadas para IPv4 e IPv6 para facilitar la transición de una red solo IPv4 a un diseño de red solo IPv6

Seguridad

La serie de conmutadores HPE Aruba Networking CX 6300 viene con un módulo de plataforma confiable (TPM) incorporado para la integridad de la plataforma. Esto garantiza que el proceso de arranque se inicie desde una combinación confiable de conmutador y HPE Aruba Networking AOS-CX. Otras características de seguridad incluyen:

- AOS-CX utiliza criptografía validada FIPS 140-2 para proteger la información confidencial

- Soporte de lista de control de acceso (ACL) tanto para IPv4 como para IPv6, permite filtrar el tráfico para evitar que usuarios no autorizados accedan a la red. Controla el tráfico de entrada para ahorrar recursos de reglas, puede denegar o permitir el reenvío del tráfico. Las reglas pueden basarse en un encabezado de capa 2 o en un encabezado de protocolo de capa 3.

- Las ACL también proporcionan filtrado basado en el campo IP, la dirección IPv4 o host de origen/destino y el número de puerto TCP/UDP de origen/destino por VLAN o por puerto.

- La inscripción a través de Trompeta Segura (EST) permite la inscripción de equipos de confianza, lo que permite una gestión empresarial más segura de PKI.

- Servidor de soporte de autenticación remota (RADIUS)

- El sistema de control de acceso del controlador de acceso al terminal (TACACS+) ofrece una herramienta de autenticación sencilla TCP con cifrado de la solicitud de autenticación completa, lo que proporciona seguridad adicional

- Seguridad de acceso y administración para autenticación de firma y hora del equipo para acceso administrativo. Se pueden utilizar RADIUS o TACACS+ para proporcionar autenticación de usuario directa. Además, TACACS+ también puede proporcionar servicios de autorización de administrador.

- Controles de policía centralizados en ambos puertos de velocidad entre puertos de usuario para proteger o descargar la CPU contra paquetes DoS

- Admite múltiples métodos de autenticación de usuarios. Utiliza un solicitante IEEE 802.1X en el cliente junto con un servidor RADIUS para autenticar de acuerdo con los estándares de la industria.

- La autenticación basada en web mediante el portal cautivo en ClearPass es compatible con casos de uso como acceso de invitados y para dispositivos que no admiten 802.1x o autenticación MAC.

- Admite autenticación de cliente basada en MAC

- Los esquemas de autenticación IEEE 802.1X, web y MAC simultáneos por puerto del switch aceptan hasta 32 sesiones de autenticaciones IEEE 802.1X, web y MAC.

- La protección DHCP bloquea paquetes DHCP de servidores DHCP no autorizados, evitando ataques de denegación de servicio.

- El acceso de administración seguro ofrece cifrado seguro de todos los métodos de acceso (CLI, GUI o MIB) a través de SSHv2, SSL y/o SNMPv3.

- La protección de la CPU del conmutador proporciona protección automática contra el tráfico de red malicioso que intenta apagar el conmutador

- La Base de datos de IP de confianza de DHCPv4 es una función de seguridad de IDHP diseñada para controlar puertos del conmutador. Solo autoriza únicamente el tráfico DHCP

- La ACL basada en dispositivo permite la implementación de una política de seguridad de acceso altamente granular y flexible y una asignación de VLAN específica para cada usuario de red autenticado.

- La protección de puerto STP BPDU bloquea las unidades de datos de protocolo de puente (BPDU) en los puertos que no requieren BPDU, evitando ataques de BPDU falsificados

- El Network Instance de IP funciona con la protección DHCP para bloquear el tráfico de hosts no autorizados, evitando la suplantación de direcciones de origen IP.

- La protección ARP dinámica bloquea las transmisiones ARP desde hosts no autorizados, evitando escuchas o robo de datos de la red.

- STP root guard protege el puente raíz de ataques mal diseñados o errores de configuración

- La seguridad del puerto permite el acceso solo a direcciones MAC específicas que el administrador puede configurar o especificar.

- El bloqueo de direcciones MAC evita que determinadas direcciones MAC configuradas conectándose a la red

- El filtrado del puerto de origen permite que solo los puertos específicos se comuniquen entre sí

- Secure Shell (SSH) cifra todos los datos transmitidos para un acceso CLI remoto seguro a través de redes IP

- Secure Sockets Layer (SSL) cifra todo el tráfico HTTP, lo que permite un acceso seguro a la GUI de administración basada en navegador en el conmutador.

- FTP seguro permite la transferencia segura de archivos hacia y desde el conmutador, protege contra descargas de archivos no autorizados y copias y actualizaciones de archivos de configuración del conmutador

- La función de autenticación unificada garantiza que los dispositivos de infraestructura importantes, como los teléfonos IP, tengan acceso a la red incluso en ausencia de un servidor RADIUS

- MAC Pinning permite que los dispositivos heredados que no admiten 802.1X mantengan autenticados al flujo las direcciones MAC del cliente al puerto hasta que los clientes cierren sesión o se desconecten

- El panel de seguridad ofrece un panel de seguridad procesable cuando los usuarios inician sesión en el conmutador

- RadSec permite que los datos de contabilidad y autenticación RADIUS se transmitan de forma segura y confiable a través de redes públicas

- VLAN privada (PVLAN) proporciona aislamiento de tráfico entre usuarios en la misma

CONSORCIO EMDOC
EMDOC
CONSORTIO
Santo Domingo RD

VLAN; normalmente, un puerto de conmutador solo puede comunicarse con los miembros de la misma comunidad VLAN o un enlace ascendente independientemente del ID de VLAN o la dirección MAC de destino, lo que amplía la seguridad de la red al restringir la comunicación entre pares para mitigar una variedad de ataques maliciosos.

- Auto VLAN Creation automatiza la creación de VLAN en conmutadores de acceso para clientes autenticados.

- La retransmisión inteligente de DHCP permite que el agente de retransmisión DHCP utilice direcciones IP secundarias cuando el servidor DHCP no responde al mensaje DHCPOFFER

- IEEE 802.1AE MACsec encripta toda la seguridad de conmutador a conmutador y de conmutador a host en un enlace entre dos puertos mediante cifrado y autenticación estándar, disponible en puertos de enlace ascendente y descendente

Visibilidad y seguridad avanzadas: los clientes pueden optar por actualizar su conmutador con un paquete de características avanzadas de HPE Aruba Networking CX para desbloquear los siguientes beneficios para su negocio.

- Visibilidad profunda y reconocimiento de aplicaciones con NetEdge Insights, incluida la recopilación granular de grandes cantidades de datos con búsqueda, clasificación e informes.

- Control y aplicación de políticas basadas en roles y aplicaciones con la capacidad de reconocer más de 3600 aplicaciones en 22 categorías y tomar medidas. Las acciones de política incluyen eliminar, comercializar y reflejar.

- Postura de seguridad de red reforzada con servicios de cifrado WAN MACsec y soporte para política refleja.

Multidifusión

- IGMP Snooping permite que varias VLAN reutilicen el mismo ancho de multidifusión IPv4, lo que reduce la demanda de ancho de banda de la red al reducir múltiples flujos a cada VLAN.

- Descubrimiento de enrutador de multidifusión (MRD) permite el descubrimiento de sondeos de multidifusión IPv4 compatible con MLD v1 y v2

- La multidifusión independiente del protocolo (PIM) define modos de multidifusión IPv4 e IPv6 para permitir la transmisión de uno a muchos y de muchos a muchos de información. admite el modo disperso (SM) de PIM, la multidifusión específica de fuente (SSM) y el modo denso (DM) tanto para IPv4 como para IPv6.

- El Protocolo de administración de grupos de Internet (IGMP) utiliza multidifusión de cualquier fuente (ASM) para administrar redes de multidifusión IPv4; admite IGMPv1, v2 y v3

- El protocolo de enrutamiento de árbol de expansión (MSTP) evita bucles en la ruta de multidifusión a nivel de capa de enlace

- MSDP para implementar el protocolo de una fuente (anycast) que proporciona redundancia y capacidades de carga compartida

Convergencia

- Direccionamiento de multidifusión IP multicapa mediante PIM Sparse, Source-Specific Multicast (SSM) y Dense para enrutar el tráfico de multidifusión IP.

- La detección de calidad basada en UDP (BQD) ayuda a encontrar rápidamente fallas en la ruta de multidifusión IP

- La multidifusión independiente del protocolo para IPv6 admite casos de uso de transmisión de medios de muchos a muchos, como IPTV a través de redes IPv6

- LLDP-MED (Media Endpoint Discovery) define una extensión estándar de LLDP que almacena valores para parámetros como QoS y VLAN para configurar automáticamente dispositivos de red como teléfonos IP.

- Las asignaciones de PoE admiten múltiples métodos (asignación por clase, con LLDP y LLDP-MED) para asignar energía PoE para una administración de energía y ahorros de energía más eficientes.

- Configuración automática de VLAN para una implementación sin problemas con RADIUS estándar y LLDP-MED para configurar automáticamente una VLAN para teléfonos IP

- CDP (solo CX) y CDPv2 para configurar teléfonos IP habilitados

Información adicional

- Apoyo a iniciativas ecológicas para las regulaciones RoHS (EN 50581:2012) y WEEE

- Todos los conmutadores Cx 6300 cumplen con EAA

El cliente primero, el cliente al final
Cuando su red es importante para su negocio, entonces su negocio necesita el respaldo de los servicios de soporte de redes HPE Aruba. Asóciese con HPE Aruba

Conecte con expertos en productos para aumentar la productividad de su equipo, aumentar el ritmo de innovación, las iniciativas de cultura y optimizar sistemas para operación de alertas.

Los servicios de soporte Foundational Care para HPE Aruba Networking incluyen acceso prioritario a los ingenieros del Centro de asistencia técnica (TAC) de HPE Aruba Networking las 24 horas del día, los 7 días de la semana, los 365 días del año, hardware flexible y opciones de soporte móvil, y cobertura total para los productos HPE Aruba Networking. Los conmutadores HPE Aruba Networking con suscripciones asignadas a HPE Aruba Networking Central se benefician de la opción de soporte de hardware adicional (next-preview).

HPE Aruba Networking Pro Care agrega acceso rápido a los ingenieros senior de TAC de HPE Aruba Networking, quienes son asignados como un único punto de contacto para la gestión de casos, lo que reduce el tiempo dedicado a abordar y resolver problemas.

Para obtener detalles completos sobre Foundational Care y HPE Aruba Networking Pro Care, visite https://www.arubanetworks.com/support-services/

Garantía, servicios y soporte. Garantía limitada de por vida; consulte https://www.arubanetworks.com/support-services/product-warranties/ para obtener información sobre garantías y soporte incluido con la compra de su producto

Para obtener información más detallada sobre la versión y las características de cualquier HPE Aruba Networking AOS-CX, visite el portal de documentación del software del conmutador AOS-CX

Explore y compare las funciones del switch para cada plataforma y versión de software en el Navegador de funciones del switch HPE/Aruba Networking

Para versiones de software y documentación, consulte https://asp.arubanetworks.com/downloads

Para obtener información sobre soporte y servicios, visite https://www.arubanetworks.com/support-services/sales/

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

341

Especificaciones técnicas

	Conmutador HPE Aruba Networking CX 6300M 48p SR5.5P/4SR/4SR-Class8 PoE 4p HPE FAN Core (R9B91A)	HPE Aruba Networking 6300M 24p HPE Smart Rate 1G/2.5G/5G/10G Class8 PoE y conmutador 2p 5G y 2p 25G (R8S89A)	HPE Aruba Networking 6300M 48p HPE Smart Rate 1G/2.5G/5G ClassB PoE y conmutador 2p 5G y 2p 25G (R8S90A)
Descripción	48 puertos SmartRate 100M/Puertos PoE 1G/2.5G/5G/10G BaseT Clase 8 que admiten hasta 90 W por puerto (MACsec) 4 puertos 1/10/25G/40G/100G QSFP/ QSFP28 (MACsec) Soporta los estándares PoE IEEE 802.3at, 802.3at y 802.3bt (hasta 90W) 1 puerto de consola USB-C (mayor prioridad que el puerto de consola RJ45) 1 x puerto de consola RJ45 1 x OOBM 1X puerto host USB tipo A 1X Adaptador Bluetooth opcional para usar con la aplicación móvil AOS-CX	24 puertos SmartRate 100M/Puertos PoE 1G/2.5G/5G/10G BaseT Clase 6 que admiten hasta 60 W por puerto (MACsec) 2x10G/25G/50G Puertos SFP 2 puertos SFP 1G/2.5G (MACsec) Soporta estándares PoE IEEE 802.3af, 802.3at y 802.3bt (hasta 60W) 1 puerto de consola USB-C 1 puerto de consola RJ1 puerto OOBM 1 puerto host USB tipo A 1 adaptador Bluetooth opcional para usar con la aplicación CX Mobile	48 puertos SmartRate 100M/Puertos PoE 1G/2.5G/5G BaseT Clase 8 que admiten hasta 60 W por puerto (MACsec) 2x10G/25G/50G Puertos SFP 2 puertos SFP 1G/2.5G (MACsec) Soporta estándares PoE IEEE 802.3af, 802.3at y 802.3bt (hasta 90W) 1 puerto de consola USB-C 1 puerto de consola RJ1 puerto OOBM 1 puerto host USB tipo A 1 adaptador Bluetooth opcional para usar con la aplicación CX Mobile
Accesorios recomendados	Fuente de alimentación recomendada: JL086A JL487A JL670A JL758A Potencia máxima de PoE: 3600W	Fuente de alimentación recomendada: JL086A JL087A JL670A JL758A Potencia total máxima de PoE: 2880W	Fuente de alimentación recomendada: JL086A JL087A JL670A JL758A Potencia máxima de PoE: 2400W
Garantía			

Características físicas

Dimensiones	(Al) 4,4 cm x (An) 44,2 cm x (Pr) 47,2 cm (1,73" x 17,4" x 18,6")	(Al) 4,4 cm x (An) 44,2 cm x (Pr) 38,5 cm (1,73" x 17,4" x 15,2")	(Al) 4,4 cm x (An) 44,2 cm x (Pr) 38,5 cm (1,73" x 17,4" x 15,2")
Peso de configuración	7,75 kg (17,09 libras)	5,24 kg (11,69 libras)	5,48 kg (12,05 libras)

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

Especificaciones técnicas

	Conmutador HPE Aruba Networking CX 6300M, 48p SFP56 y 4p QSFP28 Classic Port 4p 10/25G MACsec (R0M49A)	HPE Aruba Networking 6300M, 24p HPE SmartRate 1G/2.5G/5G/10G CL6 PoE y conmutador 2p 50G y 2p 25G (R8S86A)	HPE Aruba Networking 6300M, 48p HPE SmartRate 1G/2.5G/5G CL8 PoE y conmutador 2p 50G y 2p 25G (R8S90A)
Especificaciones adicionales			
UPC	ARM Cortex® A72 de cuatro núcleos a 1,8 GHz	ARM Cortex® A72 de cuatro núcleos a 1,8 GHz	ARM Cortex® A72 de cuatro núcleos a 1,8 GHz
memoria y flash	8 GB DDR4 32 GB eMMC	8 GB DDR4 32 GB eMMC	8 GB DDR4 32 GB eMMC
Ranura de expansión	Ninguna	Ninguna	Ninguna
Actuación			
Capacidad de conmutación de la matriz	176 Gbit/s	760 Gbps	760 Gbps
Capacidad de reenvío (paquetes de tamaño mixto)	Hasta 96 mpps	Hasta 565 mpps	Hasta 565 mpps
Latencia promedio (paquetes UDP de 64 bytes)		1 Gbps: 4,24 µSeg; 10Gbps: 1,50µSeg; 25Gbps: 2,91 µSeg; 50Gbps: 3,49 µSeg	1Gbps: 4,24µSeg; 10Gbps: 1,50µSeg; 25Gbps: 2,91 µSeg; 50Gbps: 3,49µSeg
Tamaño de búfer	10 microsegundos	10 microsegundos	10 microsegundos
Rendimiento sostenido de ráfagas	Hasta 10 ms con transceptores de largo alcance	Hasta 10 ms con transceptores de largo alcance	Hasta 10 ms con transceptores de largo alcance
Ancho de banda de apilamiento	400 Gbps	200 Gbps	200 Gbps
Interfaces virtuales compatibles (SVI máximo)	1 024	1 024	1 024
Tabla de hosts IPv4 (ARP)	49 152	49,152	49 152
Tabla de hosts IPv6 (ND)	49 152	49,152	49.152
Rutas de unidifusión IPv4	61.000	61.000	61 000
Rutas de unidifusión IPv6	61.000	61,000	61 000
Rutas de multidifusión IPv4	8.192	8.192	8.192
Rutas de multidifusión IPv6	8.192	8.192	8 192
Capacidad de tabla MAC	32.768	32.768	32.768
Grupos IGMP	8.192	8.192	8.192
Grupos MLD	8.192	8.192	8.192
Entradas de ACL IPv4/IPv6/MAC (ingreso)	20.480/5.120/20.480	20 480/5.120/20.480	20 480/5.120/20.480
Entradas de ACL IPv4/IPv6/MAC (salida)	8.192/2.048/8.192	8.192/2.048/8.192	8.192/2 048/8 192
VRF	256	256	256

[redacted]

[redacted]

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

Especificaciones técnicas

	[illegible] HPE Aruba Networking CX 6300M 48p 1GbE 4SFP/SFP+ Switch Pod de 1800 MACsec (R8S91A)	HPE Aruba Networking 6300M 24p HPE Smart Rate 1G/2.5G/5G/10G CL6 PoE y conmutador 2p 50G y 2p 25G (R8S89A)	HPE Aruba Networking 6300M 48p HPE Smart Rate 1G/2.5G/5G CL6 PoE y conmutador 2p 50G y 2p 25G (R8S90A)
Ambiental			
Temperatura de funcionamiento	32 °F a 113 °F (0 °C a 45 °C) hasta 5000 pies. Reducción de potencia de 1 grado C por cada 1000 pies de 5000 pies a 10 000 pies Puede soportar excursiones a 131 °F (55 °C) por períodos cortos de tiempo	32 °F a 113 °F (0 °C a 45 °C) hasta 5000 pies. Reducción de potencia de 1 grado C por cada 1000 pies de 5000 pies a 10 000 pies Puede soportar excursiones a 131 °F (55 °C) por períodos cortos de tiempo.	32 °F a 113 °F (0 °C a 45 °C) hasta 5000 pies. Reducción de potencia de 1 grado C por cada 1000 pies de 5000 pies a 10 000 pies Puede soportar excursiones a 131 °F (55 °C) por períodos cortos de tiempo.
Humedad relativa de funcionamiento	Del 5 % al 95 % a 104 °F (40 °C) sin condensación	Del 5 % al 95 % a 104 °F (40 °C) sin condensación	Del 5 % al 95 % a 104 °F (40 °C) sin condensación
No operativo	-40 °F a 158 °F (-40 °C a 70 °C) hasta 15,000 pies	-40 °F a 158 °F (-40 °C a 70 °C) hasta 15,000 pies	-40 °F a 158 °F (-40 °C a 70 °C) hasta 15,000 pies
Temperatura relativa no operativa y humedad de 24 h de almacenamiento	5 % a 95 % a 149 °F (65 °C) sin condensación	5 % a 95 % a 149 °F (65 °C) sin condensación	5 % a 95 % a 149 °F (65 °C) sin condensación
Altitud de funcionamiento	10,000 pies (3,04 km) máx.	10,000 pies (3,04 km) máx.	10,000 pies (3,04 km) máx.
Altitud máxima no operativa	15,000 pies (4,6 km) máx.	15,000 pies (4,6 km) máx.	15,000 pies (4,6 km) máx.
Acústico	Potencia sonora, LWAd = 4,8 belios Presión sonora, LpAm (espectador) = 33,7 dB	Potencia sonora, LWAd = 4.5 belios Presión sonora, Lpam (espectador) = 33,0 dB	Potencia sonora, LWAd = 5,0 belios Presión sonora, Lpam (espectador) = 33,0 dB
Flujo de aire predeterminado	De adelante y de lado a lado	De adelante y de lado a lado	De adelante y de lado a lado
Características eléctricas			
Frecuencia	50/60 Hz	50/60 Hz	50/60 Hz
Voltaje de entrada	110 V-120 V/208 V-240 V entrada de CA	110 V-120 V/208 V-240 V	110 V-120 V/208 V-240 V
Consumo de energía (230 VCA)			

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

Especificaciones técnicas

	Conmutador HPE Aruba Networking CX 6300M 48p 5G/10 PTP/MACsec Clase B Port 4p 10G MacSec (S0E91A)	HPE Aruba Networking 6300M 24p SFP Smart Rate 1/2.5/5/10G CL6 PoE y conmutador 2p 50G y 2p 25G (R8S89A)	HPE Aruba Networking 6300M 48p HPE Smart Rate 1/2.5/5G CL6 PoE y conmutador 2p 50G y 2p 25G (R8S90A)
Seguridad			
Incluye EE. UU., Canadá, Europa y global mundo	Europa: EN 62368-1:2014 +A11:2017 Ed 62368-1:2020 +A1:2020 EE. UU.: UL 62368-1 2.ª ed. CAN: CSA-C22.2 No. 62368-1-19 2.ª ed. Mundial: IEC 62368-1:2014(2.ª edición) IEC 62368-1:2018(3.ª edición) Taiwán: CNS 15598-1:2020	Europa: EN 62368-1:2014 +A11:2017 2.ª ed. EN 62368-1:2020 +A1:2020 3.ª ed. BS EN 62368-1:2014 + A11:2017 2.ª edición BS EN 62368-1:2020 + A1:2020 3.ª edición EE. UU.: UL 62368-1 2.ª edición, CAN/CSA-C22.2 No. 62368-1-14 2.ª ed. Mundial: IEC 60950-1:2005 + Am1:2009 Cumplimiento con todas las ediciones nacionales calificadas IEC 62368-1:2014 2.ª edición con todas las desviaciones nacionales calificadas IEC 62368-1:2018 3.ª edición con todas las desviaciones nacionales calificadas*	Europa: EN 62368-1:2014 +A11:2017 2.ª ed. EN 62368-1:2020 +A11:2020 3.ª ed. BS EN 62368-1:2014 + A11:2017 2.ª edición BS EN 62368-1:2020 + A11:2020 3.ª edición EE. UU.: UL 62368-1 2.ª edición, CAN/CSA-C22.2 No. 62368-1-14 2.ª ed. Mundial: IEC 60950-1:2005 + Am1:2009 Cumplimiento con todas las ediciones nacionales calificadas IEC 62368-1:2014 2.ª edición con todas las desviaciones nacionales calificadas IEC 62368-1:2018 3.ª edición con todas las desviaciones nacionales calificadas*
Emisiones			
Incluye EE. UU., Canadá, Europa y global mundo	Europa: EN 55032:2015 +A11:2020, Clase A EN 55035:2017+A11:2020 EN IEC 61000-3-2:2019+A1:2021 EN 61000-3-3:2013+A2:2021 EE. UU.: FCC 47 CFR; parte 15 subparte B, Clase A CAN: ICES-003(A)/NMB-003, edición 7:2020, Clase A Japón: VCCI-CISPR 32:2016, Clase A Taiwán: CNS 15936:2018, Clase A AUS/NZ: AS/NZS CISPR 32:2015+A1:2020, Clase A en todo el mundo: CISPR 32:2015/AMD1:2019, Clase A CISPR 35:2016	Europa: EN 55032:2015 +A11:2020, Clase A EN 55035:2017 +A11:2020 EN 61000-3-2:2014, Clase A EN 61000-3-3:2013 EE. UU.: FCC CFR47 Parte 15:2014, Clase A ICES-003 Clase A Mundial: VCCI, Clase A CISPR 32 Clase A CISPR 35:2016	Europa: EN 55032:2015 +A11:2020, Clase A EN 55035:2017 +A11:2020 EN 61000-3-2:2014, Clase A EN 61000-3-3:2013 EE. UU.: FCC CFR47 Parte 15:2014, Clase A ICES-003 Clase A Mundial: VCCI Clase A CISPR 32 Clase A CISPR 35:2016
Láseres			
Incluye EE. UU., Canadá, Europa y global mundo	EN 60825-1:2014 +A11:2021 / IEC 60825-1:2014 Productos láser Clase 1 / Laser Klasse 1 / Classe 1 (Aplicable a accesorios: transceptores ópticos/direccionales)	EN 60825-1:2014 / IEC 60825-1:2014 Clase 1 Productos láser clase 1 / Laser Klasse 1 (Aplicable para accesorios - Óptica sólo transceptores)	EN 60825-1:2014 / IEC 60825-1:2014 Clase 1 Productos láser Clase 1 / Laser Klasse 1 (Aplicable para accesorios - Óptica sólo transceptores)

CONSORCIO EMDOC
EMDOC
Santo Domingo, R.D.

Especificaciones técnicas

	Conmutador HPE Aruba Networking CX 6300M 48p SFP56 4p SFP+/28 Clase8 PoE 4p 1060 MACsec (R8S89A)	HPE Aruba Networking 6300M 24p HPE Smart Rate 1G/2.5G/5G CL6 PoE y conmutador 2p 10G y 2p 25G (R8S88A)	HPE Aruba Networking 6300M 48p HPE Smart Rate 1G/2.5G/5G CL8 PoE y conmutador 2p 10G y 2p 25G (R8S89A)
Inmunidad			
Genérico	CISPR 35	CISPR 35	CISPR 35
ES	EN 55035:2017	EN 55035:2017	EN 55035:2017
ESD	CEI 61000-4-2	CEI 61000-4-2	CEI 61000-4-2
Irradiado	CEI 61000-4-3	CEI 61000-4-3	CEI 61000-4-3
EFT/Ráfaga	CEI 61000-4-4	CEI 61000-4-4	CEI 61000-4-4
Aumento	CEI 61000-4-5	CEI 61000-4-5	CEI 61000-4-5
Realizado	CEI 61000-4-6	CEI 61000-4-6	CEI 61000-4-6
Campo magnético de frecuencia de potencia	CEI 61000-4-8	CEI 61000-4-8	CEI 61000-4-8
Caídas e interrupciones de tensión	CEI 61000-4-11	CEI 61000-4-11	CEI 61000-4-11
Armónicos	IEC 61000-3-2:2018+A1:2020; EN IEC 61000-3-2:2019+A1:2021	IEC 61000-3-2, EN 61000-3-2	IEC 61000-3-2, EN 61000-3-2
Parpadeo	CEI/EN 61000-3-3:2013+A2:2021	IEC 61000-3-3, EN 61000-3-3	IEC 61000-3-3, EN 61000-3-3
Montaje y envolvente			
	[illegible]	[illegible]	[illegible]

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

Especificaciones técnicas

	HPE Aruba Networking 6300M 48SR5 6p Class8 PoE y 8p Class6 PoE Switch (compatible con HPE Smart Rate 8G/1.5G/5G y 2p 50G y 2p 10G LRM (R8S91A)	Soporte HPE Aruba Networking CX 6300 2p sFP+ LRM y controlador MACsec 2p 5G y 2p 2G (R8S92A)
Descripción	48 puertos Smartrate 100M/1/2.5/5/10GBASE-T PoE Class8 de 60W (2.5G/5G que admiten hasta 90W por puerto en los puertos 1 a 12 y hasta 80 W por puerto en los puertos 13 a 48 (MACsec) 2x10G/25G/50G sFP28 puertos SFP 2 puertos SFP 10G/1.0G (1 RM + MACsec) Soporta estándares PoE IEEE 802.3af, 802.3at y 802.3bt (hasta 90W) 1 puerto de consola USB-C * puerto de consola RJ-45 * puerto OOBM 1x puerto host USB tipo A 1x dongle Bluetooth para usar con la aplicación CX Mobile	24 puertos 10/1/0.5 SFP+ (LRM + MACsec) 2x 10G/25G/50G Puertos SFP 2 puertos SFP 10GM 2.5G (MACsec) 1 puerto de consola USB-C 1 puerto de consola RJ 1 puerto OOBM 1x puerto host USB tipo A dongle Bluetooth para usar con la aplicación CX Mobile
[illegible]	[illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] JL086A JL087A JL670A JL758A [illegible]	[illegible] [illegible] [illegible] [illegible] [illegible] JL658A [illegible]
[illegible]	[illegible] [illegible] [illegible] [illegible] [illegible] [illegible]	[illegible] [illegible] [illegible] [illegible] [illegible] [illegible]
Características físicas		
Dimensiones	(Alto) 4,4 cm x (Ancho) 44,2 cm x (Prof) 38,9 cm (1.73" x 17,4" x 15,3")	(Alto) 4.4 cm x (ancho) 44.2 cm x (Prof) 38.5 cm (1.73" x 17,4" x 15,2")
Peso de configuración	5.4 kg (12,00 libras)	4.85 kg (10.70 libras)

[illegible]

[illegible]

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

Especificaciones técnicas

	HPE Aruba Networking 6300M 48p Clase4 PoE y 8p Clase6 PoE Conmutador HPE Smart Rate 2.5G/5G y 2p 50G y 2p 10G (R8N91A)	Soporte HPE Aruba Networking 6300M 48p SFP+ 8MB y conmutador MACsec 2p 50G y 2p 25G (R8S92A)
Especificaciones adicionales		
CPC	ARM Cortex A72 de cuatro núcleos a 1,8GHz	ARM Cortex A72 de cuatro núcleos a 1,8 GHz
Memoria y flash	8 GB DDR4 32 GB eMMC	8 GB DDR4 32 GB eMMC
Búfer de paquetes	4 mega	4 mega
Actuación		
Capacidad de conmutación fabric/backplane	720 Gbps	720 Gbps
Capacidad de reenvío de conmutación	535 Mpps	Mismo que producto
Latencia promedio (paquetes UDP de 64 bytes)	1Gbps: 4,24µSeg 10Gbps: 1,50µSeg 25Gbps: 2,91µSeg 50Gbps: 3,49µSeg	1Gbps: 4,24µSeg 10Gbps: 1,50µSeg 25Gbps: 2,91µSeg 50Gbps: 3,49µSeg
Tamaño de pila	10 miembros	10 miembros
Distancia máxima de cobre/fibra	Hasta 10Gbps con transceptores de largo alcance	Hasta 10Gbps con transceptores de largo alcance
Ancho de banda de la pila	200 Gbps	200 Gbps
Enrutadores virtuales compatibles (máx.)	1,024	1,024
Tabla de hosts IPv4 (ARP)	49.152	49.152
Tabla de hosts IPv6 (NDP)	49.152	49.152
Rutas de unidifusión IPv4	61.000	61.000
Rutas de unidifusión IPv6	61.000	61.000
Rutas de multidifusión IPv4	8.192	8.192
Rutas de multidifusión IPv6	8.192	8.192
Capacidad de la tabla MAC	32.768	32.768
Grupos IGMP	8.192	8.192
Grupos MLD	8.192	8.192
Entradas de ACL IPv4/IPv6/MAC (ingreso)	20.480/5.120/20.480	20.480/5.120/20.480
Entradas de ACL IPv4/IPv6/MAC (salida)	8.192/2.048/8.192	8.192/2.048/8.192
VRF	255	256

[illegible]

[illegible]

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

Especificaciones técnicas

	HPE Aruba Networking 6200M 12p Class4 PoE y 36p Class6 PoE Conmutador HPE Smart Rate 1G/2.5G/5G y 2p 50G y 4p 10G (R8S91A)	Soporte HPE Aruba Networking 6200M 24p gig+ 4SFP+ Lite y conmutador JL676A 6300F 24p SFP56 (R8S92A)
Ambiente		
Temperatura de funcionamiento[1][2]	32 °F a 113 °F (0 °C a 45 °C) hasta 5000 pies Reducción de potencia 1 grado C por cada 1000 pies de 5001 pies a 10 000 pies.	32 °F a 113 °F (0 °C a 45 °C) hasta 5000 pies2 Reducción de potencia 1 grado C por cada 1000 pies de 5000 pies a 10 000 pies.
	Puede soportar descargas de 131 °F (55 °C) por períodos controlados de tiempo.	Puede soportar descargas de 131 °F (55 °C) por períodos controlados de tiempo.
		La expansión de SSC no es compatible cuando se instala 10GBASE-LR/ER.
		Cuando se implementan 1XG-R1 y 10GBASE-LR/ER serializados, toda la redundancia del ventilador solo se admite hasta 104 °F (40 °C) 5000 pies
Humedad relativa de funcionamiento	Del 5 % al 95 % a 104 °F (40 °C) sin condensación	Del 5 % al 95 % a 104 °F (40 °C) sin condensación
No operativo	-40 °F a 158 °F (-40 °C a 70 °C) hasta 15,000 pies	-40 °F a 158 °F (-40 °C a 70 °C) hasta 15,000 pies
Humedad relativa sin funcionamiento (sin formación de condensación)	5 % a 95 % a 149 °F (65 °F) sin condensación	5 % a 95 % a 149 °F (65 °C) sin condensación
Altitud de funcionamiento	10,000 pies (3,04 km) máx.	10 000 pies (3,04 km) máx.
Altitud máxima no operativo	15,000 pies (4,6 km) máx.	15 000 pies (4,6 km) máx.
Acústico	Potencia sonora (LWAd) = 4,9 bellios Presión sonora, Lpam (espectador) = 31,6 dB	Potencia sonora (LWAd) = 4,6 bellios Presión sonora, Lpam (espectador) = 30,1 dB
Flujo de aire principal	De adelante a detrás (I a E)	De adelante a detrás (I a E)
Características eléctricas		
Frecuencia	50/60 Hz/60Hz	50Hz/60Hz
Tensión nominal	Corriente alterna (CA) 110 V-120 V/208 V-240 V Ajuste de tensión de línea, 60 V/208 V Tensión de entrada, 100 V-127 V	Tensión nominal (rms): 100 a 240 V
Corriente de entrada máxima (con fuente de alimentación)	Tensión de alimentación 100 V CA 11 A Tensión de alimentación 200 V CA 5,5 A Tensión de alimentación 240 V CA 4,6 A	Corriente máxima: 2,5 A
Consumo de energía (ESM VCP)	Configuración probada Inactivo: 111 W Tasa de cable en 100 Mb: 118 W Tasa de cable en 1 Gb: 120 W Inactivo: 114 W Tasa de cable en 100 Mb: 118 W Tasa de cable en 1 Gb: 120 W Tasa de pulso del 100 %: 173 W	Inactivo: 87 W Tasa de pulso de 100 %: 131 W

CONSORCIO EMDOC
EMDOC
Santo Domingo R.D.

Especificaciones técnicas

	HPE Aruba Networking 6300M 12p Clase8 PoE y 36p Clase8 PoE Conmutador HPE Smart Rate 8SV 2.5GbE y 24 SFP y 2p 10G (R8S91A)	Soporte HPE Aruba Networking 6300M 24p SFP+ ENet y conmutador 6/ACsoc 2p 10G y 2p 25G (R8S92A)
Seguridad		
Incluye EE.UU., Canadá, Europa y todo el mundo	Europa EN 62368-1:2014 +A11:2017 2ª ed EN 62368-1:2020 +A11:2020 3ª ed. RHINO UNIDO: BS EN 62368-1:2014 + A11:2017 2.ª edición BS EN 62368-1:2020 + A11:2020 3ª edición BS. UU./Canadá UL 62368-1 2.ª edición, CAN/CSA-C22.2 No 62368-1-14 2.ª ed. Mundial IEC 60950-1:2005 + Am1:2009 + Am2:2013 con todas las diferencias nacionales conocidas IEC 62368-1:2014 2.ª edición, con todas las diferencias nacionales conocidas IEC 62368-1:2018 3.ª edición, con todas las diferencias nacionales conocidas*	Europa: EN 62368-1:2014 +A11:2017 2ª ed. EN 62368-1:2020 +A11:2020 3ª ed. RHINO UNIDO: BS EN 62368-1:2014 + A11:2017 2.ª edición BS EN 62368-1:2020 + A11:2020 3ª edición BS UU./Canadá UL 62368-1 2.ª edición, CAN/CSA-C22.2 No. 62368-1-14 2.ª ed. Mundial: IEC 60950-1:2005 + Am.:2009 + Am2:2013 con todas las desviaciones nacionales compiladas IEC 62368 1:2014 2.ª edición con todas las diferencias nacionales conocidas IEC 62368-1:2018 3.ª edición con todas las diferencias nacionales conocidas*
Emisiones		
Incluye EE.UU., Canadá, Europa y todo el mundo	Europa: EN 55032:2015 +A11:2020, Clase A EN 55035:2017 +A11:2020 EN 61000-3-2:2014, Clase A EN 61000-3-3:2013 [illegible] FCC CFR47 Parte 15:2014, Clase A ICES-003 Clase A Mundial: VCCI Clase A CISPR 32 Clase A CISPR 35:2016	Europa: EN 55032:2015 +A11:2020, Clase A EN 55035:2017 +A11:2020 EN 61000-3-2:2014, Clase A EN 61000-3-3:2013 [illegible] FCC CFR47 Parte 15:2014, Clase A ICES-003 Clase A Mundial: VCCI Clase A CISPR 32 Clase A CISPR 35:2016
Láser		
Incluye EE.UU., Canadá, Europa y todo el mundo	EN 60825-1:2014 / IEC 60825-1:2014 Clase 1 Productos láser clase 1 / Laser Klasse 1 (Aplicable para accesorios ópticos Sólo transceptores)	EN 60825-1 2014 / IEC 60825-1:2014 Clase 1 Productos láser clase 1 / Laser Klasse 1 (Aplicable para accesorios Óptico Sólo transceptores)



Especificaciones técnicas

	HPE Aruba Networking 630FM 12p Class8 PoE y 24p Class6 PoE Conmutador HPE Solution Para 10/2.5GBase-T y 2p 50G y 2p 10G (R8S91A)	Soporte HPE Aruba Networking 630M 24p SFP+ LRM y conmutador MACsec 2p 50G y 2p 25G (R8S92A)
Inmunidad		
Genérico	CISPR 35	CISPR 35
ES	EN 55035:2017	EN 55035:2017
ESD	CEI 61000-4-2	CEI 61000-4-2
Irradiado	CEI 61000-4-3	CEI 61000-4-3
Ráfaga/Transitorio	CEI 61000-4-4	CEI 61000-4-4
Aumento	CEI 61000-4-5	CEI 61000-4-5
Realizado	CEI 61000-4-6	CEI 61000-4-6
Campo magnético de frecuencia de potencia	CEI 61000-4-8	CEI 61000-4-8
Caídas e interrupciones de tensión	CEI 61000-4-11	CEI 61000-4-11
Armónicos	IEC 61000-3-2, EN 61000-3-2	IEC 61000-3-2, EN 61000-3-2
Parpadeo	IEC 61000-3-3, EN 61000-3-3	IEC 61000-3-3, EN 61000-3-3
Montaje y envolvente		
	Se requiere un mínimo de 1 ranura de expansión para instalar 1 fuente de alimentación opcional. Montaje en bastidor horizontal (incluye orejetas de montaje en bastidor de 2 postes).	Se requiere un mínimo de 1 ranura de expansión para instalar 1 fuente de alimentación opcional. Montaje en bastidor horizontal (incluye orejetas de montaje en bastidor de 2 postes).

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo R.D.

Especificaciones técnicas

	Redes HPE Aruba [illegible]	Redes HPE Aruba [illegible]	Redes HPE Aruba [illegible]	Redes HPE Aruba [illegible]
Descripción	24x puertos 10/100/1000 Puertos BaseT PoE+ soporta hasta 30W por puerto 4x1 G/10G/25G/50G Puertos SFP Soporte extensores PoE IEEE 802.3af, 802.3at 1 puerto de consola USB-C 1 puerto USB 1 puerto host USB tipo A 1 llave Bluetooth para usar con la aplicación CX Mobile	48x puertos 10/100/1000 Puertos BaseT 6x1G/10G/25G/50G Puertos SFP 1 puerto de consola USB-C 1 puerto OOBM 1 puerto host USB tipo A 1 llave Bluetooth para usar con la aplicación CX Mobile	24x puertos 10/100/1000 Puertos BaseT 4x1 G/10G/25G/50G Puertos SFP 1 puerto de consola USB-C 1 puerto OOBM 1 puerto host USB tipo A 1 llave Bluetooth para usar con la aplicación CX Mobile	48x puertos 10/100/1000 Puertos BaseT 4x1G/10G/25G/50G Puertos SFP 1 puerto de consola USB-C 1 puerto OOBM 1 puerto host USB tipo A 1 llave Bluetooth para usar con la aplicación móvil AOS-CX
[illegible]	1 compartimiento de campo [illegible] 1 ventilador reemplazable en caliente (pedido por separado) [illegible] JL086A JL087A JL670A [illegible]	2 compartimientos de campo [illegible] 1 potencia mínima suministro requerido (pedido por separado) [illegible]	2 compartimientos de campo [illegible] 1 potencia mínima suministro requerido (pedido por separado) [illegible]	2 compartimientos de campo [illegible] Par2Par adicional Solo admite fuente de alimentación JL364A PWR2Pri
[illegible]	[illegible]	[illegible]	[illegible]	[illegible] reemplazable y [illegible] Solo admite bandejas de ventilador JL671A 2wr2Pri.

Características físicas

Dimensiones	(Alto) 4,4 cm x (Ancho) 44,3 cms [illegible] (1,73" x 17,4" x 15,2")	(Alto) 4,4 cm x (Ancho) 44,3 cms [illegible] (1,73" x 17,4" x 15,2")	(Alto) 4,4 cm x (Ancho) 44,3 cm x [illegible] (1,73" x 17,4" x 15,2")	(Alto) 4,4 cm (Ancho) 44,3 cm [illegible] (1,73" x 17,4" x 15,2")
Peso de configuración	5,56 kg (12,23 libras)	3,91 kg (11,14 libras)	5,45 kg (11,97 libras)	7PSU 5,7 kg (12,5 libras) 2PSU 4,7 kg (10,3 libras)

[illegible]

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo R.D.

Especificaciones técnicas

	Redes HPE Aruba 6300M 24 puertos 1GbE Clase 4 PoE y 4 puertos SFP56	Redes HPE Aruba 6300M 48 puertos 1GbE y 4 puertos	Redes HPE Aruba 6200M 24 puertos 1GbE y 4 puertos	Redes HPE Aruba
Especificaciones adicionales				
CPU	ARM Cortex-A72 de cuatro núcleos a 1,8 GHz	ARM Cortex-A72 de cuatro núcleos a 1,8 GHz	ARM Cortex-A72 de cuatro núcleos a 1,8 GHz	ARM Cortex-A72 de cuatro núcleos a 1,8 GHz
Memoria y flash	8 GB DDR4	8 GB DDR4	8 GB DDR4	DDR4 de 8 GB eMMC de 32 GB
Búfer de paquetes	9 MB compartidos de paquetes de 9 KB	Búfer de paquetes de 8 MB Memoria	Búfer de paquetes de 8 MB Memoria	8 MB de paquetes compartidos dinámicamente Memoria
Actuación				
Capacidad de conmutación de red	448 Gbps	496 Gbps	448 Gbps	496 Gbps
Capacidad de reenvío de red	334 Mpps	369 Mpps	334 Mpps	369 Mpps
Latencia media (paquetes UDP de 64 bytes)	1Gbps: 2,30µSeg. 10Gbps: 1,46µSeg. 25Gbps: 1,90µSeg. 50 Gbps: 3,49µSeg	1Gbps: 2,28µSeg. 10Gbps: 1,46µSeg. 25Gbps: 1,90µSeg. 50 Gbps: 3,49µSeg	1Gbps: 2,28µSeg 10Gbps: 1,46µSeg. 25Gbps: 1,90µSeg. 50 Gbps: 3,49µSeg	1Gbps: 2,28µSeg 10Gbps. 1,46µSeg. 25Gbps: 1,90µSeg. 50 Gbps: 3,49µSeg
Pila de conmutación	10 miembros	10 miembros	10 miembros	10 miembros
Interconexión de agregación de pila	Hasta 40 GbE con transceptores de largo alcance	Hasta 10 GbE con transceptores de largo alcance	Hasta 10 GbE con transceptores de largo alcance	Hasta 10 GbE con transceptores de largo alcance
Rendimiento de pila de borde	200 Gbps	200 Gbps	200 Gbps	200 Gbps
Interfaces virtuales compatibles (pila dual)	1.024	1.024	1.024	1.024
Tabla de hosts IPv4 (ARP)	49.152	49.152	49.152	49.152
Tabla de hosts IPv6 (ND)	49.152	49.152	49.152	49.152
Rutas de unidifusión IPv4	61.000	61.000	61.000	61.000
Rutas de unidifusión IPv6	61.000	61.000	61.000	61.000
Rutas de multidifusión IPv4	8.192	8.192	8.192	8.192
Rutas de multidifusión IPv6	8.192	8.192	8.192	8.192
Cantidad de VLAN admitidas	32.768	32.768	32.768	32.768
Grupos IGMP	8.192	8.192	8.192	8.192
Grupos MLD	8.192	8.192	8.192	8.192
ACL IPv4/IPv6/MAC entradas (entrada)	20.480/5.120/20.480	20.480/5.120/20.480	20.480/5.120/20.480	20.480/5.120/20.480
ACL IPv4/IPv6/MAC entradas (salida)	8.192/2.048/8.192	8.192/2.048/8.192	8.192/2.048/8.192	8.192/2.048/8.192
VRF	256	256	256	256

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

Especificaciones técnicas

	Redes HPE Aruba [illegible] 24 puertos 10GBASE-T PoE y 4 puertos SFP56 Switch (Bundle)	Redes HPE Aruba 6300M 48 puertos 1GbE y [illegible]	Redes HPE Aruba 6300M 24 puertos 1GbE y [illegible]	Redes HPE Aruba [illegible] 24 puertos 1GbE PPS (Precision Time Protocol) y [illegible]
Ambiente				
Temperatura de funcionamiento	32°F a 113°F (0°C a 45°C) hasta 5000 pies. Reducción de 1 grado C por cada 1000 pies de 5000 pies a 10 000 pies. Puede soportar una excursión a 131°F (55°C) por un corto tiempo período de tiempo.	32°F a 113°F (0°C a 45°C) hasta 5000 pies. Reducción de 1 grado C por cada 1000 pies de 5000 pies a 10,000 pies. Puede soportar una excursión a 131°F (55°C) por un corto tiempo período de tiempo.	32°F a 113°F (0°C a 45°C) hasta 5000 pies. Reducción de 1 grado C por cada 1000 pies de 5000 pies a 10,000 pies. Puede soportar una excursión a 131°F (55°C) por un corto tiempo períodos de tiempo.	32°F a 113°F (0°C a 45°C) hasta 5000 pies de altitud de prueba - 1°C por cada 1000 pies de 5000 pies hasta 10000 pies
Relativo operativo Humedad	0% a 95% a 104 °F (40 °C) sin condensación	5 % a 95 % a 104 °F (40 °C) sin condensación	5 % a 95 % a 104 °F (40 °C) sin condensación	5 % a 95 % a 104 °F (40 °C) sin condensación
No operativo	-40°F a 158°F (-40°C a 70°C) hasta 15,000 pies	-40°F a 158°F (-40°C a 70°C) hasta 15,000 pies	-40°F a 158°F (-40°C a 70°C) hasta 15,000 pies	-40°F a 158°F (-40°C a 70°C) hasta 15000 pies
Almacenamiento no operativo humedad relativa	5 % a 95 % a 149 °F (65 °C) sin condensación	5 % a 95 % a 149 °F (65 °C) sin condensación	5 % a 95 % a 149 °F (65 °C) sin condensación	5 % a 95 % a 149 °F (65 °C) sin condensación
[illegible]	10,000 pies (3,04 km) máx.	10,000 pies (3,04 km) máx.	10,000 pies (3,04 km) máx.	10,000 pies (3,04 km) máx.
Altitud máxima no operativa	15,000 pies (4,6 km) máx	15,000 pies (4,6 km) máx	15,000 pies (4,6 km) máx.	15,000 pies (4,6 km) máx.
Acústico	Presión de sonido $L_{pA,d}$ 47 belios presión sonora, L_{pA}(espectador) = 20,4 dB	Presión de sonido $L_{pA,d}$ 36 belios presión sonora, L_{pA}(espectador) = 28,7 dB	Potencia de sonido $L_{pA,d}$ 44 belios Presión sonora, L_{pA}(espectador) = 28,6 dB	Potencia de sonido $L_{pA,d}$ 50 belios presión sonora, L_{pA}(espectador) = 32,5 dB [illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
Características eléctricas				
Frecuencia	50Hz/60Hz	50Hz/60Hz	50-Hz/60Hz	50Hz/60Hz
[illegible]	[illegible] 100 V-127 V/200 V-240 V [illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
Certificaciones [illegible]	-	-	-	[illegible]
Rendimiento de energía (230 VCA)	[illegible] Eficiencia del 100% 91% [illegible] Eficiencia del 100% 94% [illegible] Eficiencia del 100% 94%	[illegible] Eficiencia del 100% 94%	[illegible] Eficiencia del 100% 94%	[illegible] Eficiencia del 100% 95%

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

Especificaciones técnicas

	Redes HPE Aruba	Redes HPE Aruba	Redes HPE Aruba	Redes HPE Aruba
	6300M 24 puertos BASE-Clase A 2GE y 4 puertos SFP56	6300M 48 puertos 10GE y 4 puertos SFP56 y 4 puertos QSFP56	6300M 24 puertos MGBE y 4 puertos SFP56 y 4 puertos QSFP56	Redes HPE Aruba [illegible] puertos [illegible] y 4 puertos [illegible]
Seguridad				
	Europa: EN 60950-1:2006 +A11:2009 +A1:2010 + A12:2011 + A2:2013 EE. UU.: UL 60950-1 2ª edición Canadá: CAN/CSA-C22.2 Nº 60950-1-07 Mundial: IEC [illegible]	Europa: EN 60950-1:2006 +A11:2009 +A1:2010 + A12:2011 + A2:2013 EE. UU.: UL 60950-1 2ª edición Canadá: CAN/CSA-C22.2 Nº 60950-1-07 Mundial: IEC [illegible]	Europa: EN 60950-1:2006 +A11:2009 +A1:2010 + A12:2011 + A2:2013 EE. UU.: UL 60950-1 2ª edición. Canadá: CAN/CSA-C22.2 Nº 60950-1-07 Mundial: IEC [illegible]	Europa: EN 60950-1:2006 +A11:2009 +A1:2010 + A12:2011 + A2:2013 EN 62368-1:2014 + A11:2017 EE. UU.: UL 60950-1 2ª edición Canadá: CAN/CSA-C22.2 Nº 60950-1-07 Mundial: IEC 60950-1:2005 con todas las desviaciones nacionales y condiciones IEC 62368-1:2014 2ª edición. Taiwán: CNS 14336-1
Emisiones				
	Europa: EN 55022:2010, Clase A EN 55032:2012, Clase A EN 55024:2010 EN 61000-3-2:2014 EN 61000-3-3:2013 [illegible] FCC parte 15 Clase A Canadá ICES-003 Clase A Mundial: VCCI Clase A CISPR 22 Clase A CISPR 32 Clase A CISPR 24:2010	Europa: EN 55022:2010, Clase A EN 55032:2012, Clase A EN 55024:2010 EN 61000-3-2:2014 EN 61000-3-3:2013 [illegible] FCC parte 15 Clase A Canadá ICES-003 Clase A Mundial: VCCI Clase A CISPR 22 Clase A CISPR 32 Clase A CISPR 24:2010	Europa: EN 55022:2010, Clase A EN 55032:2012, Clase A EN 55024:2010 EN 61000-3-2:2014 EN 61000-3-3:2013 [illegible] FCC parte 15 Clase A Canadá ICES-003 Clase A Mundial: VCCI Clase A CISPR 22 Clase A CISPR 32 Clase A CISPR 24:2010	Europa: EN 55032:2015 +AC:2016, Clase A EN 55035:2017 EN 61000-3-2:2014 EN 61000-3-3:2013 [illegible] FCC 47 CFR parte 15B, Clase A Canadá: ICES-003 Clase A Mundial: VCCI Clase A CISPR 32 Ed 2.0: 2015 + CCR1:2016, Clase A CISPR 35:2016
Láseres				
	EN 60825-1:2007 / IEC 60825-1:2007 Clase 1 Productos láser clase 1 - Laser Klasse 1 [illegible]	EN 60825-1:2007 / IEC 60825-1:2007 Clase 1 Productos láser clase 1 / Laser Klasse 1 [illegible]	EN 60825-1:2007 / IEC 60825-1:2007 Clase 1 Productos láser clase 1 / Laser Klasse 1 [illegible]	EN 60825-1:2007 / IEC 60825-1:2007 Clase 1 Productos láser de clase 1/ láser clase 1 (aplicable a periféricos: transceptores ópticos únicamente)
Inmunidad				
Genérico	CISPR 24 / CISPR 35	CISPR 24 / CISPR 35	CISPR 24 / CISPR 35	CISPR 35
ES	EN 55024:2010 / EN 55035:2017	EN 55024:2010 / EN 55035:2017	EN 55024:2010 / EN 55035:2017	EN 55035:2017
ESD	CEI 61000-4-2	CEI 61000-4-2	CEI 61000-4-2	CEI 61000-4-2

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

Especificaciones técnicas

	Redes MPE Aruba (300mA) 8x puertos mGE Clase 4 PoE y 4 puertos SFP56 Interruptor (R4G2A)	Redes HPE Aruba 6300M 48 puertos 5GBT y 4 puertos SFP56 Interruptor (S3L5A)	Redes HPE Aruba 6200F 24 puertos 1GBE y 4 puertos SFP56 Interruptor (JL676A)	Redes HPE Aruba 6200F 48 puertos 1GBE y 4 puertos SFP56 Interruptor (JL677A)
Inmunidad				
Irradiado	CEI 61000-4-3	CEI 61000-4-3	CEI 61000-4-3	CEI 61000-4-3
Electrostática	CEI 61000-4-2	CEI 61000-4-2	CEI 61000-4-2	CEI 61000-4-2
Ambiental	CEI 61000-4-5	CEI 61000-4-5	CEI 61000-4-5	CEI 61000-4-5
Rastreado	CEI 61000-4-6	CEI 61000-4-6	CEI 61000-4-6	CEI 61000-4-6
Campo magnético de frecuencia industrial	CEI 61000-4-8	CEI 61000-4-8	CEI 61000-4-8	CEI 61000-4-8
Caídas de tensión y interrupciones	CEI 61000-4-11	CEI 61000-4-11	CEI 61000-4-11	CEI 61000-4-11
Armónicos	CEI 61000-3-2, EN 61000-3-2	CEI 61000-3-2, EN 61000-3-2	CEI 61000-3-2 EN 61000-3-2	CEI 61000-3-2, EN 61000-3-2
Parpadeo	CEI 61000-3-3, EN 61000-3-3	CEI 61000-3-3, EN 61000-3-3	CEI 61000-3-3 EN 61000-3-3	CEI 61000-3-3, EN 61000-3-3
Montaje y envolvente				
	gabinete del equipo.	gabinete del equipo.	gabinete del equipo.	gabinete de equipo.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

Especificaciones técnicas

	Redes HPE Aruba [illegible]	Redes HPE Aruba [illegible]	Redes HPE Aruba [illegible] (JL667A)	Redes HPE Aruba [illegible] (JL663A)
Descripción	48 puertos 10/100/1000BaseT PoE+ [illegible] 4 ranuras SFP+ 10G [illegible]	24 puertos 10/100/1000BaseT soporta hasta 30W por puerto	48 puertos 10/100/1000BaseT	24 puertos 10/100/1000BaseT
	4p 1G/10G/25G/50G Puertos SFP	4p 1G/10G/25G/50G Puertos SFP	4p 1G/10G/25G/50G Puertos SFP	4p 1G/10G/25G/50G Puertos SFP
	Soporta estándares PoE IEEE 802.3af, 802.3at	1 puerto de consola USB-C 1 puerto OOBM	1 puerto de consola USB-C 1 puerto OOBM	1 puerto de consola USB-C 1 puerto OOBM
	1 puerto de consola USB-C 1 puerto OOBM 1 puerto host USB tipo A 1 adaptador Bluetooth para usar con la aplicación CX Mobile	1 puerto host USB tipo A 1 adaptador Bluetooth para usar con la aplicación CX Mobile	1 puerto host USB tipo A 1 adaptador Bluetooth para usar con la aplicación CX Mobile	1 puerto host USB tipo A 1 adaptador Bluetooth para usar con la aplicación CX Mobile
[illegible]	Alimentación [illegible] suministro (980W)	Alimentación [illegible] suministro (750W)	Alimentación [illegible] suministro (600W)	Alimentación [illegible] suministro (600W)
	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
Características físicas				
Dimensiones	(Alto) 4,39 cm x (Ancho) 44,0 cm x [illegible] (1,73" x 17,4" x 12,9")	(Alto) 4,39 cm x (Ancho) 44,0 cm x [illegible] (1,73" x 17,4" x 12,9")	(Alto) 4,39 cm x (Ancho) 44,0 cm x [illegible] (1,73" x 17,4" x 12,9")	(Alto) 4,39 cm x (Ancho) 44,0 cm x [illegible] (1,73" x 17,4" x 12,9")
Peso de configuración	5,10 kg (11,24 libras)	4,96 kg (10,94 libras)	4,46 kg (9,83 libras)	4,36 kg (9,61 libras)
Especificaciones adicionales				
CPU	AMD Cortex™ A72 de cuatro núcleos a 1,8 GHz	ARM Cortex™ A72 de cuatro núcleos a 1,8 GHz	ARM Cortex™ A72 de cuatro núcleos a 1,3 GHz	ARM Cortex™ A72 de cuatro núcleos a 1,8 GHz
Memoria y flash	8 GB DDR4 [illegible]	8 GB DDR4 [illegible]	8 GB DDR4 [illegible]	8 GB DDR4 [illegible]
[illegible]	Memoria intermedia de paquetes de 64 MB	Búfer de paquetes de 64 MB dinámica	Búfer de paquetes de 64 MB dinámica	Búfer de paquetes de 64 MB Memoria

[illegible]

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

Especificaciones técnicas

	Redes HPE Aruba [illegible]	Redes HPE Aruba [illegible]	Redes HPE Aruba [illegible]	Redes HPE Aruba [illegible]
Actuación				
[illegible]	496 Gbps	448 Gbps	496 Gbps	448 Gbps
[illegible]	369 Mpp	334 Mpp	369 Mpp	334 Mpp
Latencia media (paquetes LIFO de 64 bytes)	1Gbps: 2.20µSeg 10Gbps: 1,46µSeg. 25Gbps: 1.90µSeg. 50 Gbps: 3,49µSeg	1Gbps: 2.28µSeg 10Gbps: 1.46µSeg. 25Gbps: 1.90µSeg. 50 Gbps: 3,49µSeg	1Gbps: 2.28µSeg. 10Gbps: 1.46µSeg. 25Gbps: 1.90µSeg. 50 Gbps: 3,49µSeg	1Gbps: 2.28µSeg 10Gbps: 1,46µSeg. 25Gbps: 1.90µSeg 50 Gbps: 3,49µSeg
[illegible]	10 miembros	10 miembros	10 miembros	10 miembros
[illegible]	Hasta 10 links con mismo protocolo de largo alcance	Hasta 10 links con [illegible]	Hasta 10 links con [illegible]	Hasta 10 links con [illegible]
[illegible]	200 Gbps	200 Gbps	200 Gbps	200 Gbps
Interfaces virtuales por switch (pila stack)	1.024	1.024	1.024	1.024
Tabla de hosts IPv4 (ARP)	49.152	49.152	49.152	49.152
Tabla de hosts IPv6 (NDP)	49.152	49.152	49.152	49.152
[illegible]	61.000	61.000	61.000	61.000
[illegible]	61.000	61.000	61.000	61.000
[illegible]	8.192	8.192	8.192	8.192
[illegible]	8.192	8.192	8.192	8.192
Capacidad de la tabla MAC	32.768	32.768	32.768	32.768
Grupos IGMP	8.192	8.192	8.192	8.192
Grupos MLD	8.192	8.192	8.192	8.192
ACL IPv4/IPv6/MAC entradas (ingreso)	20.480/5.120/20.480	20.480/5.120/20.480	20.480/5.120/20.480	20.480/5.120/20.480
ACL IPv4/IPv6/MAC entradas (salida)	8.192/2.048/8.192	8.192/2.048/8.192	8.192/2.048/8.192	8.192/2.048/8.192
VRF	256	256	256	256

[illegible]

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

Especificaciones técnicas

	Redes HPE Aruba 6300F Conmutador PoE Clase 4 de 48 puertos 1/2.5GbE y 4 puertos SFP56 (JL658A)	Redes HPE Aruba 6300F de 48 puertos 1/2.5GbE y 4 puertos SFP56 (JL659A)	Redes HPE Aruba Conmutador PoE de 24 puertos 1/2.5GbE y 4 puertos SFP56 (JL660A)	Redes HPE Aruba Conmutador PoE de 24 puertos 1/2.5GbE y 4 puertos SFP56 (JL661A)
Ambiente				
Temperatura en funcionamiento	32 °F a 113 °F (0 °C a 45 °C) hasta 5000 pies. Reducción de 1 grado C por cada 1000 pies de 5000 pies a 10,000 pies Puede soportar una excursión a 131 °F (55 °C) por un corto tiempo en períodos de tiempo.	32 °F a 113 °F (0 °C a 45 °C) hasta 5000 pies. Reducción de 1 grado C por cada 1000 pies de 5000 pies a 10 000 pies. Puede soportar una excursión a 131 °F (55 °C) para períodos cortos de tiempo.	32 °F a 113 °F (0 °C a 45 °C) hasta 5000 pies. Reducción de 1 grado C por cada 1000 pies de 5000 pies a 10 000 pies. Puede soportar una excursión a 131 °F (55 °C) para períodos cortos de tiempo.	32 °F a 113 °F (0 °C a 45 °C) hasta 5000 pies. Reducción de 1 grado C por cada 1000 pies de 5000 pies a 10 000 pies. Puede soportar una excursión a 131 °F (55 °C) para períodos cortos de tiempo.
Rango operativo humedad	Del 5 % a 95 % a 104 °F (40 °C) sin condensación	5 % a 95 % a 104 °F (40 °C) sin condensación	5 % a 95 % a 104 °F (40 °C) sin condensación	5 % a 95 % a 104 °F (40 °C) sin condensación
No operativo	-40 °F a 158 °F (-40 °C a 70 °C) hasta 15,000 pies	-40 °F a 158 °F (-40 °C a 70 °C) hasta 15,000 pies	-40 °F a 158 °F (-40 °C a 70 °C) hasta 15 000 pies	-40 °F a 158 °F (-40 °C a 70 °C) hasta 15 000 pies
Almacenamiento no operativo humedad relativa	5 % a 95 % a 149 °F (65 °C) sin condensación	5 % a 95 % a 149 °F (65 °C) sin condensación	5 % a 95 % a 149 °F (65 °C) sin condensación	5 % a 95 % a 149 °F (65 °C) sin condensación
Altitud máxima de funcionamiento	10,000 pies (3,04 km) máx.	10,000 pies (3,04 km) máx.	10 000 pies (3,04 km) máx.	10 000 pies (3,04 km) máx.
Altitud máxima no operativa	15,000 pies (4,6 km) máx.	15,000 pies (4,6 km) máx.	15 000 pies (4,6 km) máx.	15 000 pies (4,6 km) máx.
Acústico	Potencia de sonido. L_{WAd} 5,2 belios presión sonora. L_{pAm} (espectador) = 34,9 dB	Potencia de sonido. L_{WAd} 5,0 belios presión sonora. L_{pAm} (espectador) = 32,5 dB	Potencia de sonido. L_{WAd} 5,0 belios presión sonora. L_{pAm} (espectador) = 31,5 dB	Potencia de sonido L_{WAd} 4,9 belios presión sonora. L_{pAm} (espectador) = 31,6 dB
Flujo de aire operativo	De adelante a atrás	De adelante a atrás	De adelante a atrás	De adelante a atrás
Características eléctricas				
Frecuencia	50/60 Hz	50/60 Hz	50/60 Hz	50/60 Hz
Rango de voltaje operativo	100 V-120 V/200 V-240 V	100 V-120 V/200 V-240 V	100 V-120 V/200 V-240 V	100 V-120 V/200 V-240 V
Configuración de alimentación recomendada				
Certificación 80plus.org	-	-	-	
Bloque de energía (230 VCA)	Tasa de salida con 100% de carga	Tasa de salida del 90% de carga	Tasa de salida del 100% de carga	Tasa de salida del 90% de carga
Seguridad				
	Europa: EN 60950-1:2006 +A11:2009 +A1:2010 + A12:2011 + A2:2013	Europa: EN 60950-1:2006 +A11:2009 +A1:2010 + A12:2011 + A2:2013	Europa: EN 60950-1:2006 +A11:2009 +A1:2010 + A12:2011 + A2:2013	Europa: EN 60950-1:2006 +A11:2009 +A1:2010 + A12:2011 + A2:2013
	EE.UU.: UL 60950-1 2ª edición	EE.UU.: UL 60950-1 2ª edición	EE.UU.: UL 60950-1 2ª edición	EE.UU.: UL 60950-1 2ª edición
	Canadá: CAN/CSA-C22.2 Nº 60950-1-07	Canadá: CAN/CSA-C22.2 Nº 60950-1-07	Canadá: CAN/CSA-C22.2 Nº 60950-1-07	Canadá: CAN/CSA-C22.2 Nº 60950-1-07
	Mundial: IEC 60950-1:2005 con todas las desviaciones nacionales	Mundial: IEC Aplica a los productos y desviaciones nacionales	Mundial: IEC Aplica a los productos y desviaciones nacionales	Mundial: IEC 60950-1:2005 con todas las desviaciones nacionales

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

Especificaciones técnicas

	Redes HPE Aruba [illegible]	Redes HPE Aruba [illegible]	Redes HPE Aruba [illegible]	Redes HPE Aruba [illegible]
Emisiones				
	Europa: EN 55032:2010, Clase A EN 55032:2012, Clase A EN 55024:2010 EN 61000-3-2:2014 EN 61000-3-3:2013	Europa: EN 55022:2010, Clase A EN 55032:2012, Clase A EN 55024:2010 EN 61000-3-2:2014 EN 61000-3-3:2013	Europa: EN 55022:2010, Clase A EN 55032:2012, Clase A EN 55024:2010 EN 61000-3-2:2014 EN 61000-3-3:2013	Europa: EN 55022:2010, Clase A EN 55032:2012, Clase A EN 55024:2010 EN 61000-3-2:2014 EN 61000-3-3:2013
	[illegible]: FCC parte 15 Clase A	[illegible]: FCC parte 15 Clase A	[illegible]: FCC parte 15 Clase A	[illegible]: FCC parte 15 Clase A
	Canadá: CIEM-003 Clase A	Canadá: CIEM-003 Clase A	Canadá: CIEM-003 Clase A	Canadá: CIEM-003 Clase A
	Mundial: VCCI Clase A CISPR 22 Clase A CISPR 32 Clase A CISPR 24:2010	Mundial: VCCI Clase A CISPR 22 Clase A CISPR 32 Clase A CISPR 24:2010	Mundial: VCCI Clase A CISPR 22 Clase A CISPR 32 Clase A CISPR 24:2010	Mundial: VCCI Clase A CISPR 22 Clase A CISPR 32 Clase A CISPR 24:2010
Láseres				
	EN 60825-1:2007 / IEC 60825-1:2007 Clase 1 Productos láser clase 1 / Láser Clase 1 (Aplicable a accesorios [illegible])	EN 60825-1:2007 / IEC 60825-1:2007 Clase 1 Productos láser de clase 1/ láser clase 1 (aplicable a accesorios: transceptores ópticos únicamente)	EN 60825-1:2007 / IEC 60825-1:2007 Clase 1 Productos láser de clase 1/ láser clase 1 aplicable a accesorios transceptores ópticos (únicamente)	EN 60825-1:2007 / IEC 60825-1:2007 Clase 1 Productos láser de clase 1/ láser clase 1 (aplicable a accesorios: transceptores ópticos únicamente)
Inmunidad				
Generico	CISPR 24 / CISPR 35	CISPR 24 / CISPR35	CISPR 24 / CISPR 35	CISPR 24 / CISPR35
ES	EN 55024:2010 / EN 55035:2017	EN 55024:2010 / EN 55035:2017	EN 55024:2010 / EN 55035:2017	EN 55024:2010 / EN 55035:2017
ESD	CEI 61000-4-2	CEI 61000-4-2	CEI 61000-4-2	CEI 61000-4-2
[illegible]	CEI 61000-4-3	CEI 61000-4-3	CEI 61000-4-3	CEI 61000-4-3
[illegible]	CEI 61000-4-4	CEI 61000-4-4	CEI 61000-4-4	CEI 61000-4-4
[illegible]	CEI 61000-4-5	CEI 61000-4-5	CEI 61000-4-5	CEI 61000-4-5
Realizado	CEI 61000-4-6	CEI 61000-4-6	CEI 61000-4-6	CEI 61000-4-6
[illegible]	CEI 61000-4-8	CEI 61000-4-8	CEI 61000-4-8	CEI 61000-4-8
Caídas de tensión y interrupciones	CEI 61000-4-11	CEI 61000-4-11	CEI 61000-4-11	CEI 61000-4-11
Armónicos	CEI 61000-3-2, EN 61000-3-2	CEI 61000-3-2, EN 61000-3-2	CEI 61000-3-2, EN 61000-3-2	CEI 61000-3-2, EN 61000-3-2
Flagrante	CEI 61000-3-3, EN 61000-3-3	CEI 61000-3-3, EN 61000-3-3	CEI 61000-3-3, EN 61000-3-3	CEI 61000-3-3, EN 61000-3-3

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

Especificaciones técnicas

	Redes HPE Aruba	Redes HPE Aruba	Redes HPE Aruba	Redes HPE Aruba
	6300M Conmutador Bundle 24p 1 GbE de 4 puertos SFP56 y 4 puertos globales	Conmutador 6300F de 24 puertos 1 GbE y 4 puertos SFP56 (JL663A)	Switch HPE Aruba Conmutador 6300F de 48 puertos 1 GbE y 4 puertos SFP56 (JL667A)	Redes HPE Aruba Conmutador 6400F de 24 puertos 1 GbE y 4 puertos SFP56 (JL663A)
Montaje y envolvente				
	Montaje en bastidor de 19 pulgadas (incluido) o montaje en gabinete del equipo, superficie horizontal o montaje vertical (soportes de montaje en bastidor de 2 postes no incluidos)	Montaje en bastidor de 19 pulgadas (incluido) o montaje en gabinete del equipo, superficie horizontal o montaje vertical (soportes de montaje en bastidor de 2 postes no incluidos)	Montaje en bastidor de 19 pulgadas (incluido) o montaje en gabinete del equipo, superficie horizontal o montaje vertical (soportes de montaje en bastidor de 2 postes no incluidos)	Montaje en bastidor de 19 pulgadas (incluido) o montaje en gabinete del equipo, superficie horizontal o montaje vertical (soportes de montaje en bastidor de 2 postes no incluidos)

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

Especificaciones técnicas

	Redes HPE Aruba 6300M 24 puertos SFP+ y 4 ranuras para módulos de puertos mixtos	Redes HPE Aruba HPE 6300M de 48 puertos Tarifa Inteligente 12.5 Gbps Conmutador PoE Clase 6 y SFP56 de 4 puertos (JL659A)	Redes HPE Aruba HPE 6300M de 24 puertos Tarifa Inteligente 12.5 Gbps Conmutador PoE Clase 6 y SFP56 de 4 puertos (JL660A)	Redes HPE Aruba 6200F 48 puertos 10/100/1000 Conmutador PoE clase 4 y SFP56 de 4 puertos (JL661A)
Descripción	24 puertos 1G/10G SFP+ 4x1G/10G/25G Puertos SFP 56G 1 puerto de consola USB-C 1 puerto OOBM 1 puerto host USB tipo A 1 Aire Bluetooth para usar con la aplicación CX Mobile	48x puertos SmartRate 100M/1G/2,5G/5G Puertos PoE Bocit Clase 6 que admiten hasta 90 W por puerto 4x1G/10G/25G Puertos SFP 56G Soporta estándares PoE IEEE 802.3af, 802.3at y 802.3bt (hasta 60W) 1 puerto de consola USB-C 1 puerto OOBM 1 puerto host USB tipo A 1 Aire Bluetooth para usar con la aplicación CX Mobile	24 puertos RJ45 inteligente Puertos PoE RackT Clase 6 que admiten hasta 60 W por puerto 4x1G/10G/25G Puertos SFP 56G Soporta estándares PoE IEEE 802.3af, 802.3at y 802.3bt (hasta 60W) 1 puerto de consola USB-C 1 puerto OOBM 1 puerto host USB tipo A 1 Aire Bluetooth para usar con la aplicación CX Mobile	48 puertos 10/100/1000 Puertos PoE+ soporte hasta 30W por puerto 4x1G/10G/25G Puertos SFP 56G Soporte estándar PoE IEEE 802.3af, 802.3at 1 puerto de consola USB-C 1 puerto OOBM 1 puerto host USB tipo A 1 Aire Bluetooth para usar con la aplicación CX Mobile
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	1 potencia mínima suministro requerido (pedido por separado)	1 potencia mínima suministro requerido (pedido por separado)	1 potencia mínima suministro requerido (pedido por separado)	1 potencia mínima suministro requerido (pedido por separado)
[illegible]	[illegible] JL085A JL087A JL670A	[illegible] JL085A JL087A JL670A	[illegible] JL085A JL087A JL670A	[illegible] JL085A JL087A JL670A
[illegible]	[illegible] reemplazable y [illegible]	[illegible] reemplazable y [illegible]	[illegible] reemplazable y [illegible]	[illegible] reemplazable y [illegible]
Características físicas				
Dimensiones	(Alto) 4,4 cm x (ancho) 44,2 cm x [illegible] (1,73" x 17,4" x 15,2")	(Alto) 4,4 cm x (Ancho) 44,2 cm x [illegible] (1,73" x 17,4" x 15,2")	(Alto) 4,4 cm x (Ancho) 44,2 cm x [illegible] (1,73" x 17,4" x 15,2")	(Alto) 4,4 cm x (Ancho) 44,2 cm x [illegible] (1,73" x 17,4" x 15,2")
Peso de configuración	[illegible]	5,71 kg (12,6 libras)	5,06 kg (11,2 libras)	5,72 kg (12,6 libras)

[illegible]

EMDOC CONSORCIO
Santo Domingo, RD

Especificaciones técnicas

	Redes HPE Aruba 6300M 24 puertos SFP+ y conmutador SFP56 de 4 puertos (JL659A)	Redes HPE Aruba 6300M de 48 puertos SmartRate multigigabit 1/2.5/5/10 GbE Conmutador PoE Clase 6 y SFP56 de 4 puertos (JL660A)	Redes HPE Aruba 6300M de 24 puertos SmartRate multigigabit 1/2.5/5/10GbE Conmutador PoE Clase 6 y SFP56 de 4 puertos (JL658A)	Redes HPE Aruba 6300M 48 puertos 1GbE Conmutador PoE clase 4 y SFP56 de 4 puertos (JL664A)
Especificaciones adicionales				
UPC	ARM Cortex™ A72 de cuatro núcleos a 1,8 GHz	ARM Cortex™ A72 de cuatro núcleos a 1,8 GHz	ARM Cortex™ A72 de cuatro núcleos a 1,8 GHz	ARM Cortex™ A72 de cuatro núcleos a 1,8 GHz
Memoria y flash	4 GB DDR4	8 GB DDR4	8 GB DDR4	8 GB DDR4
Búfer de paquetes	Memoria compartida de paquetes de 8 MB	Búfer de paquetes de 8 MB Memoria	Búfer de paquetes de 8 MB Memoria	Búfer de paquetes de 8 MB Memoria
Actuación				
Capacidad de conmutación de matriz	880 Gbps	880 Gbps	640 Gbps	496 Gbps
Velocidad de reenvío (paquetes por segundo)	Hasta 714 Mpps	Hasta 714 Mpps	476 Mpps	369 Mpps
Latencia media (paquetes UDP de 64 bytes)	1 Gbps: 1,89 µSeg. 10Gbps: 1,45µSeg. 25Gbps: 2,85µSeg. 50 Gbps: 2,82µSeg	1Gbps: 4,34 µSeg. 10Gbps: 1,50µSeg. 25Gbps: 2,91 µSeg. 50 Gbps: 3,49µSeg	1Gbps: 4,34 µSeg. 10Gbps: 1,50µSeg 25Gbps: 2,91µSeg. 50 Gbps: 2,49µSeg	1Gbps: 2,28µSeg. 10Gbps: 1,45µSeg 25Gbps: 1,93µSeg. 50 Gbps: 1,49µSeg
Miembros de la pila	10 miembros	10 miembros	10 miembros	10 miembros
Máximo alcance de apilamiento	Hasta 10 km con transceptores de largo alcance	Hasta 10 km con transceptores de largo alcance	Hasta 10 km con transceptores de largo alcance	Hasta 10 km con transceptores de largo alcance
Ancho de banda de apilamiento	200 Gbps	200 Gbps	200 Gbps	200 Gbps
Interfaces virtuales conmutadas (plena pila)	1.024	1.024	1.024	1.024
Tabla de hosts IPv4 (ARP)	49.152	49.152	49.152	49.152
Tabla de hosts IPv6 (ND)	49.152	49.152	49.152	49.152
Rutas IPv4/IPv6	61.000	61.000	61.000	61.000
Rutas multidifusión IPv4	61.000	61.000	61.000	61.000
Rutas de multidifusión IPv4	8.192	8.192	8.192	8.192
Rutas de multidifusión IPv6	8.192	8.192	8.192	8.192
Capacidad de la tabla MAC	32.768	32.768	32.768	32.768
Grupos LAGP	8.192	8.192	8.192	8.192
Grupos MED	8.192	8.192	8.192	8.192
ACL IPv4/IPv6/MAC entradas (entrada)	20.480/5.120/20.480	20.480/5.120/20.480	20.480/5.120/20.480	20.480/5.120/20.480
ACL IPv4/IPv6/MAC entradas (salida)	8.192/2.048/8.192	8.192/2.048/8.192	8.192/2.048/8.192	8.192/2.048/8.192
VRF	256	256	256	256

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo RD

Especificaciones técnicas

	Redes HPE Aruba 6300M 24 puertos SFP+ y conmutador SFP56 de 4 puertos (JL663A)	Redes HPE Aruba [illegible] de 48 puertos [illegible] conmutador PoE Clase 6 y SFP56 de 4 puertos (JL664A)	Redes HPE Aruba [illegible] de 24 puertos [illegible] Conmutador PoE Clase 6 y SFP56 de 4 puertos (JL664A)	Redes HPE Aruba 6300M 48 puertos 1GbE Conmutador PoE Clase 4 y SFP56 de 4 puertos (JL661A)
Ambiente				
Temperatura de funcionamiento	32 °F a 113 °F (0 °C a 45 °C) hasta 5000 pies. Reducción de -1 grado C por cada 1000 pies de 5000 pies a 10 000 pies. Puede soportar una excursión a 131 °F (55 °C) para períodos cortos de tiempo. La temperatura de funcionamiento se reduce de 32 °F (0 °C) a 104 °F (40 °C) hasta 5000 pies cuando se instalan [illegible] (JL663A) o 100 GBase-[illegible].	32 °F a 113 °F (0 °C a 45 °C) hasta 5000 pies. Reducción de -1 grado C por cada 1000 pies de 5000 pies a 10 000 pies. Puede soportar una excursión a 131 °F (55 °C) para períodos cortos de tiempo.	32 °F a 113 °F (0 °C a 45 °C) hasta 5000 pies. Reducción de -1 grado C por cada 1000 pies de 5000 pies a 10 000 pies. Puede soportar una excursión a 131 °F (55 °C) para períodos cortos de tiempo. Se requiere una [illegible] para soportar la excursión.	32 °F a 113 °F (0 °C a 45 °C) hasta 5000 pies. Reducción de -1 grado C por cada 1000 pies de 5000 pies a 10 000 pies. Puede soportar una excursión a 131 °F (55 °C) para períodos cortos de tiempo.
Relativo operativo Humedad	Del 5 % al 95 % a 104 °F (40 °C) sin condensación	5 % a 95 % a 104 °F (40 °C) sin condensación	5 % a 95 % a 104 °F (40 °C) sin condensación	5 % a 95 % a 104 °F (40 °C) sin condensación
No operativo	-40 °F a 158 °F (-40 °C a 70 °C) hasta 15,000 pies	-40 °F a 158 °F (-40 °C a 70 °C) hasta 15,000 pies	-40 °F a 158 °F (-40 °C a 70 °C) hasta 15,000 pies	-40 °F a 158 °F (-40 °C a 70 °C) hasta 15,000 pies
Almacenamiento no operativo humedad relativa	5 % a 95 % a 149 °F (65 °C) sin condensación	5 % a 95 % a 149 °F (65 °C) sin condensación	5 % a 95 % a 149 °F (65 °C) sin condensación	5 % a 95 % a 149 °F (65 °C) sin condensación
[illegible]	10,000 pies (3,04 km) máx.	10,000 pies (3,04 km) máx.	10 000 pies (3,04 km) máx.	10,000 pies (3,04 km) máx.
Altitud máxima no operativo	15,000 pies (4,6 km) máx.	15 000 pies (4,6 km) máx.	15 000 pies (4,6 km) máx.	15,000 pies (4,6 km) máx.
Acústica	[illegible] L_{WAd} 4.9 belios presión sonora, L_{pAm} (espectador) = 51,0 dB	[illegible] L_{WAd} 5.5 belios presión sonora, L_{pAm} (espectador) = 30.6 dB	[illegible] L_{WAd} 5.2 belios presión sonora, L_{pAm} (espectador) = 34.2 dB	[illegible] L_{WAd} 4.7 belios presión sonora, L_{pAm} (espectador) = 29,8 dB
Flujo de aire principal	De adelante a atrás (puerto a PSU)	De adelante a atrás (puerto a PSU)	De adelante a atrás (puerto a PSU)	De adelante a atrás (puerto a PSU)
Características eléctricas				
Frecuencia	50Hz/60Hz	50Hz/60Hz	50Hz/60Hz	50Hz/60Hz
[illegible]	[illegible]	[illegible] 100 V-120 V/200 V-240 V [illegible]	[illegible] 100 V-120 V/200 V-240 V [illegible]	[illegible] 100 V-120 V/200 V-240 V [illegible]
Cumplimiento para voltajes (puestos arriba)	[illegible]	[illegible]	[illegible]	[illegible]
El consumo de energía (230 VCA)	Inactivo: 37 W [illegible]	[illegible] [illegible] Inactivo: 32 W Tasa de [illegible] del 100 % 158 W [illegible] [illegible] Inactivo: 19 W Tasa de [illegible] del 100 % 100 W [illegible] [illegible] Inactivo: 8 W Pico de [illegible] de 200 %: 207 W	[illegible] [illegible] Inactivo: 32 W Tasa de [illegible] del 100 % 158 W [illegible] [illegible] Inactivo: 19 W Tasa de [illegible] del 100 % 100 W [illegible] [illegible] Inactivo: 8 W Tasa de [illegible] del 100 % 13 W	[illegible] [illegible] Inactivo: 29 W Tasa de [illegible] del 100 % 100 W [illegible] [illegible] Inactivo: 7 W Tasa de [illegible] del 100 % 13 W

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo R.D.

Especificaciones técnicas

	Redes HPE Aruba S3500A 24 puertos SFP+	Redes HPE Aruba [illegible]	Redes HPE Aruba [illegible]	Redes HPE Aruba [illegible]
Seguridad				
	Europa: EN 60950-1:2006 +A11:2009 +A1:2010 + A12:2011 + A2:2013	Europa: EN 60950-1:2006 +A11:2009 +A1:2010 + A12:2011 + A2:2013	Europa: EN 60950-1:2006 +A11:2009 +A1:2010 + A12:2011 + A2:2013	Europa: EN 60950-1:2006 +A11:2009 +A1:2010 + A12:2011 + A2:2013
	[illegible]	[illegible]	[illegible]	[illegible]
	Canadá: CAN/CSA-C22.2 Nº 60950-1-07	Canadá: CAN/CSA-C22.2 Nº 60950-1-07	Canadá: CAN/CSA-C22.2 Nº 60950-1-07	Canadá: CAN/CSA-C22.2 Nº 60950-1-07
	Mundial: IEC [illegible]	Mundial: IEC [illegible]	Mundial: IEC [illegible]	Mundial: IEC [illegible]
Emisiones				
	Europa: EN 55022:2010, Clase A EN 55032:2012, Clase A EN 55024:2010 EN 61000-3-2:2014 EN 61000-3-3:2013	Europa EN 55022:2010, Clase A EN 55032:2012, Clase A EN 55024:2010 EN 61000-3-2:2014 EN 61000-3-3:2013	Europa: EN 55022:2010, Clase A EN 55032:2012, Clase A EN 55024:2010 EN 61000-3-2:2014 EN 61000-3-3:2013	Europa: EN 55022:2010, Clase A EN 55032:2012, Clase A EN 55024:2010 EN 61000-3-2:2014 EN 61000-3-3:2013
	[illegible] FCC parte 15 Clase A	[illegible] FCC parte 15 Clase A	[illegible] FCC parte 15 Clase A	[illegible] FCC parte 15 Clase A
	Canadá: CIEM-003 Clase A	Canadá: CIEM-003 Clase A	Canadá: CIEM-003 Clase A	Canadá: CIEM-003 Clase A
	Mundial: VCCI Clase A CISPR 22 Clase A CISPR 32 Clase A CISPR 24:2010	Mundial: VCCI Clase A CISPR 22 Clase A CISPR 32 Clase A CISPR 24:2010	Mundial: VCCI Clase A CISPR 22 Clase A CISPR 32 Clase A CISPR 24:2010	Mundial: VCCI Clase A CISPR 22 Clase A CISPR 32 Clase A CISPR 24:2010
Láser				
	EN 60825-1:2007 / IEC 60825-1:2007 Clase 1 Productos láser clase 1 / Laser Klasse 1 [illegible]	EN 60825-1:2007 / IEC 60825-1:2007 Clase 1 Productos láser clase 1 / Laser Klasse 1 [illegible]	EN 60825-1:2007 / IEC 60825-1:2007 Clase 1 Productos láser clase 1 / Laser Klasse 1 [illegible]	EN 60825-1:2007 / IEC 60825-1:2007 Clase 1 Productos láser clase 1 / Laser Klasse 1 [illegible]

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

Especificaciones técnicas

	Redes HPE Aruba 6300M (24 puertos SFP+ y conmutador SFP56 de 4 puertos (JL659A)	Redes HPE Aruba HPE 6300M de 48 puertos Tarifa Inteligente 1/2.5/5/10GbE Conmutador PoE Clase 6 y SFP56 de 4 puertos (JL660A)	Redes HPE Aruba HPE 6300M de 24 puertos Tarifa Inteligente 1/2.5/5/10GbE Conmutador PoE Clase 6 y SFP56 de 4 puertos (JL658A)	Redes HPE Aruba 6300M de 48 puertos 1GbE Conmutador PoE clase 4 y SFP56 de 4 puertos (JL661A)
Inmunidad				
Genérico	CISPR 24 / CISPR 35	CISPR 24 / CISPR 35	CISPR 24 / CISPR 35	CISPR 24 / CISPR 35
ESD	EN 55024:2010 / EN 55035:2017	EN 55024:2010 / EN 55035:2017	EN 55024:2010 / EN 55035:2017	EN 55024:2010 / EN 55035:2017
ESD	CEI 61000-4-2	CEI 61000-4-2	CEI 61000-4-2	CEI 61000-4-2
Irradiado	CEI 61000-4-3	CEI 61000-4-3	CEI 61000-4-3	CEI 61000-4-3
RF inducido	CEI 61000-4-4	CEI 61000-4-4	CEI 61000-4-4	CEI 61000-4-4
Sobretensión	CEI 61000-4-5	CEI 61000-4-5	CEI 61000-4-5	CEI 61000-4-5
Realzado	CEI 61000-4-6	CEI 61000-4-6	CEI 61000-4-6	CEI 61000-4-6
Campo magnético de frecuencia industrial	CEI 61000-4-8	CEI 61000-4-8	CEI 61000-4-8	CEI 61000-4-8
Caídas de tensión y interrupciones	CEI 61000-4-11	CEI 61000-4-11	CEI 61000-4-11	CEI 61000-4-11
Armónicos	CEI 61000-3-2, EN 61000-3-2	CEI 61000-3-2, EN 61000-3-2	CEI 61000-3-2 EN 61000-3-2	CEI 61000-3-2, EN 61000-3-2
Parpadeo	CEI 61000-3-3, EN 61000-3-3	CEI 61000-3-3, EN 61000-3-3	CEI 61000-3-3, EN 61000-3-3	CEI 61000-3-3, EN 61000-3-3
Montaje y envolvente				
	gabinete del equipo. Superficie horizontal	gabinete del equipo. superficie horizontal	gabinete del equipo. superficie horizontal	gabinete del equipo. Superficie horizontal

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo RD

Especificaciones técnicas

	Conmutador HPE Aruba Networking 6300L 48p Smart Rate 10G/2.5G/5G Class8 PoE 2p 50G y 2p 10G LRM L2 (S3L77A)	Conmutador HPE Aruba Networking 6300L 24p Smart Rate 10/2.5G/5G/NG Class6 PoE 4p 25G y 2p 25G L3 (S3L75A)	Conmutador HPE Aruba Networking 6300L 48p Smart Rate 10/2.5G/5G Class6 PoE 2p 50G y 2p 25G L3 (S3L76A)
Descripción	48x puertos SmartRate 100M/1G/2.5G/5G PoE BASE-T Clase 8 de 10/2.5G/5G que admiten hasta 90W por puerto en los puertos 1 a 12 y hasta 60W por puerto en los puertos 13 a 48 (MACSec) 2 puertos SFP de 10G/25G/50G 2 puertos SFP 1G/10G (MACsec) Soporta estándares PoE IEEE 802.3af, 802.3at y 802.3bt (hasta 90W) 1 puerto de consola USB-C 1 puerto de consola RJ45 1 OOBM 1x puerto host USB tipo A se adaptador Bluetooth opcional para usar con la aplicación móvil AOS-CX	24x puertos SmartRate 100M/1G/2.5G/5G PoE 1G/2.5G/5G/10G BASE-T Clase 6 que admiten hasta 60W por puerto (MACsec) 2x10G/25G/50G Puertos SFP 2 puertos SFP 10G/25G (MACsec) Soporta estándares PoE IEEE 802.3af, 802.3at y 802.3bt (hasta 60W) 1 puerto de consola USB-C 1 puerto de consola RJ1 puerto OOBM 1 conector host USB tipo A 1 adaptador Bluetooth opcional para usar con la aplicación CX Mobile	48x puertos SmartRate 10/2.5G/5G BASE-T Clase 6 que admiten hasta 90W por puerto (MACsec) 2x 10G/25G/50G Puertos SFP 2 puertos SFP 10G/25G (MACsec) Soporta estándares PoE IEEE 802.3af, 802.3at, y 802.3bt (hasta 90W) 1 puerto de consola USB-C 1 puerto de consola RJ1 puerto OOBM 1 puerto host USB tipo A 1 adaptador Bluetooth opcional para usar con la aplicación CX Mobile
[illegible]	[illegible]	[illegible]	[illegible]
	[illegible] JL086A JL087A JL670A JL758A Potencia máxima de PoE: [illegible]W	[illegible] JL086A JL087A JL670A JL758A Suministro máximo de PoE: 2880W	[illegible] JL086A JL087A JL670A JL758A Suministro máximo de PoE: 2880W
[illegible]	[illegible]	[illegible]	[illegible]
Características físicas			
Dimensiones	(Alto) 4.4 cm x (Ancho) 44.2 cm x (Pr) 36.5 cm (1.73" x 17.4" x 14.37")	40.0 cm (1.73" x 17.4" x 15.7")	38.5 cm (1.73" x 17.4" x 15.2")
Peso de configuración	5.47 kg (12.06 libras)	5.26 kg (11.60 libras)	5.49 kg (12.10 libras)

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

367

Especificaciones técnicas

	Conmutador HPE Aruba Networking 6300L 48p Smart Rate 10/2,5/5/50 ClassBUN PoE 2p 500 y 2p 165 LRM L3 (R9L77A)	Conmutador HPE Aruba Networking 6300L 24p Smart Rate 1G/2,5G/5G/10G Class6 PoE 2p 500 y 2p 250 L3 Swit (R9L78A)	Conmutador HPE Aruba Networking 6300L 48p Smart Rate 1G/2,5/5G Class8 PoE 2p 500 y 2p 250 L3 (R9L79A)
Especificaciones adicionales			
CPU	ARM Cortex® A72 de cuatro núcleos a 2,0 GHz	ARM Cortex® A72 de cuatro núcleos a 1,6 GHz	ARM Cortex® A72 de cuatro núcleos a 2,0 GHz
Memoria y flash	8 GB DDR4 32 GB eMMC	8 GB DDR4 32 GB eMMC	8 GB DDR4 32 GB eMMC
Búfer de paquetes	16 búferes	16 búferes	16 búferes
Actuación			
Capacidad de conmutación de matriz	720 Gbps	480 Gbps	480 Gbps
Capacidad de reenvío/tasa de reenvío	535 Mpps	[illegible]	[illegible]
Latencia promedio (paquetes LIFO de 64 bytes)	1Gbps: 4,24µSeg 10Gbps: 1,5Mµ Seg. 25Gbps: 2,01µSeg. 50 Gbps: 3,49 segundos	1Gbps: 4,24µSeg 10Gbps: 1,50 µSeg 25Gbps: 2,01µSeg. 50 Gbps: 3,49 segundos	1Gbps: 4,24µSeg 10Gbps: 1,50µSeg 25Gbps: 2,01µSeg. 50 Gbps: 3,49 segundos
Miembros de la pila	10 miembros	10 miembros	10 miembros
Distancias admitidas de apilamiento	Hasta 10 km con transceptores de largo alcance	Hasta 10 km con transceptores de largo alcance SFP+ o SFP28	Hasta 10 km con transceptores de largo alcance
Ancho de banda de la pila	200 Gbps	200 Gbps	200 Gbps
Interfaces virtuales (VIF) admitidas (sin DVR)	1.024	1.024	1.024
Tabla de hosts IPv4 (ARP)	49.152	49.152	49.152
Tabla de hosts IPv6 (ND)	49.152	49.152	49.152
Rutas de unidifusión IPv4	61.000	61.000	61.000
Rutas de unidifusión IPv6	61.000	61.000	61.000
Rutas de PBR (Mejor) IPv4			
Rutas de multidifusión IPv6			
Capacidad de tabla MAC	32.768	32.768	32.768
Grupos IGMP			
Grupos MLD			
Entradas de ACL IPv4/IPv6/MAC (ingreso)	20.480/5.120/20.480	20.480/5.120/20.480	20.480/5.120/20.480
Entradas de ACL IPv4/IPv6/MAC (salida)	8.192/2.048/8.192	8.192/2.048/8.192	8.192/2.048/8.192
VRF	1 VRF predeterminado, 1 VRF de gestión	1 VRF predeterminado, 1 VRF de gestión	1 VRF predeterminado, 1 VRF de gestión

[illegible]

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

368

Especificaciones técnicas

	Conmutador HPE Aruba Networking 6300L 48p Smart Rate 10/2.5G/5G/1G Class6 PoE 2p 50G y 2p 10G LRM L3 (S3L77A)	Conmutador HPE Aruba Networking 6300L 24p Smart Rate 10/2.5G/5G/1G Class6 PoE 2p 50G y 2p 25G L3 (S3L75A)	Conmutador HPE Aruba Networking 6300L 48p Smart Rate 10/2.5G/5G Class6 PoE 2p 50G y 2p 25G L3 (S3L74A)
Ambiente			
Temperatura de funcionamiento	32 °F a 113 °F (0 °C a 45 °C) hasta 5000 pies. Reducción de potencia -1 grado C por cada 1000 pies de 5000 pies a 10 000 pies Puede soportar excursiones a 131 °F (55 °C) por períodos cortos de tiempo.	32 °F a 113 °F (0 °C a 45 °C) hasta 5000 pies. Reducción de potencia -1 grado C por cada 1000 pies de 5000 pies a 10 000 pies. Puede soportar excursiones a 131 °F (55 °C) por períodos cortos de tiempo.	32 °F a 113 °F (0 °C a 45 °C) hasta 5000 pies. Reducción de potencia -1 grado C por cada 1000 pies de 5000 pies a 10 000 pies. Puede soportar excursiones a 131 °F (55 °C) por períodos cortos de tiempo
Humedad relativa de funcionamiento	Del 5 % al 95 % a 104 °F (40 °C) sin condensación	Del 5 % al 95 % a 104 °F (40 °C) sin condensación	Del 5 % al 95 % a 104 °F (40 °C) sin condensación
No operativo	-40 °F a 158 °F (-40 °C a 70 °C) hasta 15,000 pies	-40 °F a 158 °F (-40 °C a 70 °C) hasta 15,000 pies	-40 °F a 158 °F (-40 °C a 70 °C) hasta 15,000 pies
Humedad relativa no operativa	5 % a 95 % a 149 °F (65 °C) sin condensación	5 % a 95 % a 149 °F (65 °C) sin condensación	5 % a 95 % a 149 °F (65 °C) sin condensación
Altitud máxima de funcionamiento	10,000 pies (3,04 km) máx.	10,000 pies (3,04 km) máx.	10,000 pies (3,04 km) máx.
Altitud máxima no operativa	15 000 pies (4,6 km) máx.	15,000 pies (4,6 km) máx	15,000 pies (4,5 km) max.
Acústico	Potencia sonora, LWAd = 4,9 belios Presión sonora, LpAm (espectador) = 32,6 dB	Potencia sonora, LWAd = 4,9 belios Emisión sonora, LpAm (espectador) = 34,0 dB	Potencia sonora, LWAd = 5,0 belios Presión sonora, LpAm (espectador) = 34,4 dB
Flujo de aire general	De adelante y de lado a atrás	De adelante y de lado a atrás	De adelante y de lado a atrás
Características eléctricas			
Frecuencia	50Hz/60Hz	50Hz/60Hz	50Hz/60Hz
Voltaje de entrada	110 V-120 V/208 V-240 V	110 V-120 V/208 V-240 V	110 V-120 V/208 V-240 V
Consumo de energía (230 VCA)			



Especificaciones técnicas

	Conmutador HPE Aruba Networking 6200M 48p Smart Rate 1G/2.5G/5G Class6/6 PoE 2p 50G y 2p 10G LRM L3 (S3L77A)	Conmutador HPE Aruba Networking 6300M 24p Smart Rate 1G/2.5G/5G/10G Class6 PoE 2p 50G y 2p 25G L3 (S3L75A)	Conmutador HPE Aruba Networking 6300M 48p Smart Rate 1G/2.5G/5G Class6 PoE 2p 50G y 2p 25G L3 (S3L76A)
Seguridad			
Incluye EE. UU., Canadá, Europa y todo el mundo	Europa: EN 62368-1:2014 + A11:2017 2ª Ed. EN 62368-1:2020 +A11:2020 3.ª ed. Reino Unido: BS EN 62368-1:2014 + A11:2017 Norteamérica: BS EN 62368-1:2014 + A11:2017 2.ª edición BS EN 62368-1:2020+A11:2020 3.ª edición EE. UU./Canadá: UL 62368-1 2.ª edición, CAN/CSA-C22.2 No. 62368-1-14 2.ª ed. 62368-1-19 3.ª ed. Mundial: Se cumple con todas las ediciones nacionales de cada grupo regional y país enumerados	Europa: EN 62368-1:2014 +A11:2017 2ª ed. EN 62368-1:2020 +A11:2020 3.ª ed. Norteamérica: BS EN 62368-1:2014 + A11:2017 2.ª edición BS EN 62368-1:2020+ A11:2020 3.ª edición EE. UU./Canadá: UL 62368-1 2.ª edición, CAN/CSA-C22.2 No. 62368-1-14 2.ª ed. Mundial: IEC 60950-1:2005 + Am1:2009 + Am2:2013 con todas las diferencias nacionales IEC 62368-1:2018 3.ª edición con todas las desviaciones nacionales	Europa: EN 62368-1:2014 +A11:2017 2ª ed. EN 62368-1:2020 +A11:2020 3.ª ed. Norteamérica: BS EN 62368-1:2014 + A11:2017 2.ª edición BS EN 62368-1:2020+ A11:2020 3.ª edición EE. UU./Canadá: UL 62368-1 2.ª edición, CAN/CSA-C22.2 No. 62368-1-14 2.ª ed. 62368-1-19 3.ª ed. Mundial: IEC 60950-1:2005 + Am1:2009 + Am2:2013 con todas las diferencias nacionales IEC 62368-1:2018 3.ª edición con todas las desviaciones nacionales
Emisiones			
Incluye EE. UU., Canadá, Europa y todo el mundo	Europa: EN 55032:2015 +A11:2020, Clase A EN 55035:2017 +A11:2020 EN 61000-3-2:2014, Clase A EN 61000-3-3:2013 Norteamérica: FCC CFR47 Parte 15:2014, Clase A ICES-003 Clase A Mundial: VCCI Clase A CISPR 32 Clase A CISPR 35:2016	Europa EN 55032:2015 +A11:2020 Clase A EN 55035:2017 +A11:2020 EN 61000-3-2:2014, Clase A EN 61000-3-3:2013 Norteamérica: FCC CFR47 Parte 15:2016, Clase A ICES-003 Clase A Mundial: VCCI Clase A CISPR 32 Clase A CISPR 35:2016	Europa: EN 55032:2015 +A11:2020, Clase A EN 55035:2017 +A11:2020 EN 61000-3-2:2014, Clase A EN 61000-3-3:2013 Norteamérica: FCC CFR47 Parte 15:2014, Clase A ICES-003 Clase A Mundial: VCCI Clase A CISPR 32 Clase A CISPR 35:2016
Láseres			
Incluye EE. UU., Canadá, Europa y todo el mundo	EN 60825-1:2014 +A11:2021/ IEC 60825-1:2014 Clase 1 Productos láser de clase 1 Láser Clase 1 (aplicable a accesorios: transceptores ópticos únicamente)	EN 60825-1:2014 / IEC 60825-1:2014 Clase 1 Productos láser clase 1 / Laser Klasse 1 (Aplicable para accesorios: Óptico Sólo transceptores)	EN 60825-1:2014 / IEC 60825-1:2014 Clase 1 Productos láser clase 1 / Laser Klasse 1 (Aplicable para accesorios: Óptico Sólo transceptores)

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

Especificaciones técnicas

	Conmutador HPE Aruba Networking 6300L 48p Smart Rate 4p 1/2.5/5/10G Class6 PoE 2p 50G y 2p 10G 1RU L3 (S0L77A)	Conmutador HPE Aruba Networking 6300L 24p Smart Rate 4p 1/2.5/5/10G Class6 PoE 2p 50G y 2p 25G L3 (S0L75A)	Conmutador HPE Aruba Networking 6300L 48p Smart Rate 10/2.5/5G Class6 PoE 2p 50G y 2p 25G L3 (S0L78A)
Normativas			
Genérico	CISPR 35	CISPR 35	CISPR 35
ES	EN 55035:2017+A11:2020	EN 55035:2017+A11:2020	EN 55035:2017+A11:2020
ESD	CEI 61000-4-2	CEI 61000-4-2	CEI 61000-4-2
Irradiado	CEI 61000-4-3	CEI 61000-4-3	CEI 61000-4-3
[illegible]	CEI 61000-4-4	CEI 61000-4-4	CEI 61000-4-4
[illegible]	CEI 61000-4-5	CEI 61000-4-5	CEI 61000-4-5
Realizado	CEI 61000-4-6	CEI 61000-4-6	CEI 61000-4-6
Campo magnético de frecuencia industrial	CEI 61000-4-8	CEI 61000-4-8	CEI 61000-4-8
Caídas e interrupciones de tensión	CEI 61000-4-11	CEI 61000-4-11	CEI 61000-4-11
Armónicos	IEC 61000-3-2, EN 61000-3-2	IEC 61000-3-2, EN 61000-3-2	IEC 61000-3-2, EN 61000-3-2
Parpadeo	IEC 61000-3-3, EN 61000-3-3	IEC 61000-3-3, EN 61000-3-3	IEC 61000-3-3, EN 61000-3-3
Montaje y envolvente			
	[illegible]	[illegible]	[illegible]

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

Estándares y protocolos

- Descubrimiento de terminales de medios LLDP ANSI/TIA-1057/LLDP-MED
- Protección DoS de la CPU
- Mecanismo Bootstrap Router (BSR) para PIM, PIM MAG
- borrador-ietf-xxx-mtc
- IEEE 802.1AB-2005
- IEEE 802.1ak-2007
- Agregación de enlaces IEEE 802.1AX-2008
- Puentes MAC IEEE 802.1D
- Prioridad IEEE 802.1p
- VLAN IEEE 802.1Q
- Múltiples árboles de expansión IEEE 802.1
- IEEE 802.1t-2001
- Clasificación de VLAN IEEE 802.1v por protocolo y puerto
- Reconfiguración rápida IEEE 802.1w del árbol de expansión
- IEEE 802.3ab 1000BASE-T
- Protocolo de control de agregación de enlaces (LACP) IEEE 802.3ad
- IEEE 802.3ae 10 Gigabit Ethernet
- Alineación IPv4 a través de Ethernet IEEE 802.3at
- Alineación IPv6 a través de Ethernet IEEE 802.3at
- Alineación a través de Ethernet IEEE 802.3in
- Dispositivos de eficiencia energética IEEE IEEE 802.3az
- Control de flujo IEEE 802.3x
- IEEE 802.3z 1000BASE-X
- Requerido RFC 1122 para hosts de Internet - Capas de comunicaciones
- Convenio RFC 1215 para definir trampas para uso con SNMP
- Mensajes de descubrimiento de enrutador ICMP RFC 1256
- Protocolo TFTP RFC 1350 (revisión 2)
- RFC 1393 Traceroute usando una opción IP
- Interacción: RFC 1403 BGP OSPF
- RFC 1519 CIDR
- Extensiones BOOTP RFC 1542
- RFC 1583 OSPF Versión 2
- RFC 1591 Estructura y delegación del sistema de nombres de dominio
- RFC 1657 Definiciones de objetos administrados para BGP-4 usando SMIv2
- RFC 1772 Aplicación del protocolo Border Gateway en Internet
- Requisitos RFC 1812 para enrutadores IP versión 4
- RFC 1918 Asignación de direcciones para Internet privada
- Atributo de comunidades BGP RFC 1997
- RFC 1998 Una aplicación del atributo de comunidad BGP en enrutamiento multihogar
- RFC 2131 DHCP
- Opciones de DHCP RFC 2132 y extensiones de proveedor BOOTP
- RFC 2236 IGMP
- RFC 2328 OSPF Versión 2
- Asignaciones de direcciones de multidifusión IPv6 RFC 2375
- RFC 2385 Protección de sesiones BGP mediante la opción de firma TCP MD5
- Arquitectura de seguridad RFC 2401 para el protocolo de Internet
- Encabezado de autenticación IP RFC 2402
- Autenticación de flujo de ruta RFC 2439 BGP
- Especificación del protocolo de Internet RFC 2460, versión 6 (IPv6)
- RFC 2464 Transmisión de IPv6 a través de redes Ethernet
- RFC 2545 Uso de extensiones multiprotocolo BGP-4 para enrutamiento entre dominios IPv6
- RFC 2576 (Coexistencia entre SNMP V1, V2, V3)
- RFC 2579 (Convenciones de texto SMIv2)
- RFC 2580 (Conformidad SMIv2)
- RFC 2710 Descubrimiento de escucha de multidifusión (MLD) para IPv6
- Opción de alerta de enrutador IPv6 RFC 2711
- RFC 2787 Definiciones de objetos administrados para la redundancia del enrutador virtual Protocolo
- Capacidades de actualización de sesión RFC 2918 para BGP-4
- Definiciones RFC 2925 de objetos administrados para operaciones de búsqueda, rastreo y Ping remoto (sólo Ping)
- MIB de multidifusión entrante del protocolo RFC 2934 para PIM
- MIB RFC 3019 MLDv1
- Opción de información del agente de retransmisión DHCP RFC 3046
- RFC 3056 Conexión de Dominios IPv6 a través de Nubes IPv4
- RFC 3065 Confederación de Sistemas Autónomos para BGP
- RFC 3068 Un prefijo Anycast para la retransmisión 6to4
- sFlow del anuncio del enrutador mediante OSPF RFC 3137
- RFC 3376 IGMPv3
- RFC 3416 (Operaciones de protocolo SNMP V2)
- RFC 3417 (Mapeos de transporte SNMP)
- Base de información de gestión (MIB) RFC 3418 para el protocolo simple de gestión de red (SNMP)
- RFC 3484 Selección de dirección predeterminada para IPv6
- RFC 3509 Implementaciones alternativas de enrutadores fronterizos de área OSPF
- RFC 3575 Consideraciones de la IANA para RADIUS
- RFC 3623 Reinicio elegante de OSPF
- RFC 3768 VRRP
- RFC 3810 Descubrimiento de escucha de multidifusión versión 2 (MLDv2) para IPv6
- Modo denso PIM RFC 3973
- MIB RFC 4022 para TCP
- MIB RFC 4113 para UDP
- RFC 4213 Mecanismos de transición básicos para hosts y enrutadores IPv6
- RFC 4251 El protocolo Secure Shell (SSH)
- Autenticación RFC 4252 SSHv2
- Capa de transporte RFC 4253 SSHv2
- Conexión RFC 4254 SSHv2

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo RD

- RFC 4271 A Protocolo de puerta de enlace fronteriza (BGP-4)
- RFC 4273 Definiciones de objetos administrados para BGP-4
- Arquitectura de direccionamiento RFC 4291 IP versión 6
- MIB de tabla de reenvío de IP RFC 4292
- RFC 4293 Base de información de gestión para el Protocolo de Internet (IP)
- Atributo de comunidades extendidas (RFC 4360 BGP
- RFC 4419 Intercambio de claves para SSH
- RFC 4443 ICMPv6
- Reflexión de ruta BGP RFC 4456: una alternativa al iBGP interno de malla completa (IBGP)
- Subredes RFC 4486 para mensajes de notificación de cese BGP
- Conmutador de vigilancia ICMP y MLD RFC 4541
- Autenticación/confidencialidad RFC 4552 para OSPFv3
- Modo dispersa de PIM RFC 4601
- Multidifusión de fuente específica RFC 4607 para IP
- RFC 4675 VLAN de RADIO y Prioridad
- RFC 4724 Mecanismo de reinicio elegante para BGP
- Extensiones multiprotocolo RFC 4760 para BGP-4
- Descubrimiento de vecinos IPv6 RFC 4861
- Configuración automática de dirección de estado IPv6 RFC 4862
- RFC 4940 Consideraciones de IANA para OSPF
- RFC 5065 Confederación de Sistemas Autónomos para BGP
- RFC 5095 Desuso de encabezados de enrutamiento tipo 0 en IPv6
- RFC 5187 OSPFv3 Reinicio correcto
- RFC 5340 OSPF v3 para IPv6
- Protocolo Syslog RFC 5424
- Anuncio de capacidades RFC 5492 con BGP-4
- RFC 5519 (MLD v2) de gestión de membresía de grupo de multidifusión
- RFC 5701 Dirección IPv6 Atributo de comunidad extendido 2GP específico
- RFC 5722 Manejo de fragmentos de IPv6 superpuestos
- RFC 5798 VRRPv3 (IPv4 y IPv6 modo de anexación y compartición de subsegundo)
- Detección de reenvío bidireccional RFC 5880
- RFC 5905 Protocolo de tiempo de red versión 4: especificación de protocolos y algoritmos
- RFC 6620 FCFS SAVI
- Anuncio de enrutador auxiliar OSPF RFC 6987
- RFC 7047 El protocolo abierto de actualización de bases de datos vSwitch
- Capacidad de actualización de ruta mejorada RFC 7313 para BGP-4
- Protocolo de datagramas de usuario RFC 768
- Protocolo TFTP RFC 783 (revisión 2)
- RFC 791 IP
- RFC 792 ICMP
- RFC 793 TCP
- Ventana RFC 813 y estrategia de reconocimiento en TCP
- Algoritmos de reensamblaje de datagramas IP RFC 815
- Descubrimiento de MTU de ruta RFC 4821 para IP multicast
- RFC 826 ARP
- RFC 879 TCP tamaño máximo de segmento y temas relacionados
- RFC 896 Control de congestión en redes IP/TCP
- Subredes de Internet RFC 917
- RFC 919 Radiodifusión de datagramas de Internet
- RFC 922 Difusión de datagramas de Internet en presencia de subredes (IP_BROAD)
- Resolución de direcciones de host múltiple RFC 925
- RFC 951 BOOTP
- RFC 1027 Proxy ARP
- SNMPv1/v2c/v3
- Descubrimiento de vecinos IPv6 RFC 4861
- Configuración automática de direcciones sin estado IPv6 RFC 4862
- Rec. UIT-T G.8032/Y.1344, marzo de 2010
- RFC 1757 Base de información de gestión de monitoreo remoto de redes
- 2,5GBASE-T (IEEE 802.3bz-2016), 2.5G/5G NBASE-T
- 10GBASE-T (IEEE 802.3an-2006)
- Ethernet de 25 Gigabit (IEEE 802.3 para 2016, 802.3cc-2017)
- Ethernet de 50 Gigabit (IEEE 802.3cd-2018)
- RFC 3101 OSPF Opción de Sin Longitud zeroLength
- RFC 4750 OSPFv2 MIB soporte parcial sin SetMIB

Redes HPE Aruba

Interruptores CX 6300 y accesorios

Detalle de modelos

- Conmutador HPE Aruba Networking CX 6300M 48p SR1G PTP/AVB Class8 PoE 4p 100G MACsec (S0E91A)
- Conmutador HPE Aruba Networking CX 6300M 48p SR1G PTP/AVB Class8 PoE 4p 100G MACsec NAR (S0X44A)
- HPE Aruba Networking 6300M 24p HPE Smart Rate 1G/2.5G/5G/10G Class6 PoE y conmutador 2p 50G y 2p 25G (R8S89A)
- HPE Aruba Networking 6300M 48p HPE Smart Rate 1G/2.5G/5G Class6 PoE y conmutador 2p 50G y 2p 25G (R8S90A)
- HPE Aruba Networking 6300M 48SFP 2p Class6 PoE y 8p Class6 PoE Conmutador compatible con HPE Smart Rate 1G/2.5G/5G y 2p 50G y 2p 10G LRM (R8S91A)
- Compatibilidad con HPE Aruba Networking 6300M 24p SFP+ LRM y conmutador MACsec 2p 50G y 2p 25G (R8S92A)
- Conmutador HPE Aruba Networking 6300M SFP+ de 24 puertos y SFP56 de 4 puertos (R9S8A)
- Conmutador HPE Aruba Networking 6300M de 48 puertos HPE Smart Rate 1/2.5/5GBASE-T Class 6 PoE y SFP56 de 4 puertos (R9S9A)
- Conmutador HPE Aruba Networking 6300M de 24 puertos HPE Smart Rate 1/2.5/5GBASE-T Class 6 PoE y SFP56 de 4 puertos (R9S6A)

COMERCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

- Conmutador HPE Aruba Networking 6300M de 48 puertos, 1 GbE Clase 4 PoE y SFP56 de 4 puertos (JL661A)
- Conmutador HPE Aruba Networking 6300M de 24 puertos 1 GbE Clase 4 PoE y 4 puertos SFP56 (JL662A)
- Conmutador HPE Aruba Networking 6300M de 48 puertos, 1 GbE y 4 puertos SFP56 (JL663A)
- Conmutador HPE Aruba Networking 6300M de 24 puertos, 1 GbE y 4 puertos SFP56 (JL664A)
- Conmutador HPE Aruba Networking 6300F de 48 puertos, 1 GbE Clase 4 PoE y SFP56 de 4 puertos (JL665A)
- Conmutador HPE Aruba Networking 6300F de 24 puertos 1 GbE Clase 4 PoE y 4 puertos SFP56 (JL666A)
- Conmutador HPE Aruba Networking 6300F de 48 puertos, 1 GbE y 4 puertos SFP56 (JL667A)
- Conmutador HPE Aruba Networking 6300F de 24 puertos, 1 GbE y 4 puertos SFP56 (JL668A)
- Fuente de alimentación puerto HPE Aruba Networking serie de 48 puertos, 1 GbE y 4 puertos SFP56, 2 bandejas ventiladas y 1 fuente de alimentación (JL762A)

Switches de conmutación apilables

- Conmutador HPE Aruba Networking 6300L 24p Smart Rate 1G/2.5G/5G/10G Class8 PoE 2p 50G y 2p 25G L2 (S3L75A)
- Conmutador HPE Aruba Networking 6300L 48p Smart Rate 1G/2.5G/5G Class8 PoE 2p 50G y 2p 25G L2 (S3L76A)
- Conmutador HPE Aruba Networking 6300L 48p Smart Rate 1G/2.5G/5G Class8 PoE 2p 50G y 2p 10G LRM L2 (S3L77A)

Fuentes de alimentación

- Fuente de alimentación HPE Aruba Networking X371 de 12 VCC, 250 W, 100-240 VCA (JL085A)
- Fuente de alimentación HPE Aruba Networking X372 54 VCC 480 W 100-240 V CA (JL086A)
- Fuente de alimentación HPE Aruba Networking X372 54 VCC 1050 W 110-240 V CA (JL087A)
- Fuente de alimentación HPE Aruba Networking X372 54 VCC 1600 W 110-240 V CA (JL670A)
- Fuente de alimentación de alimentación a puerto HPE Aruba Networking X371 de 12 VCC 250 W, 100-240 V CA (JL084A)
- Fuente de alimentación HPE Aruba Networking 630W 250 W 36-72 VCC (JL759A)
- Redes HPE Aruba 6300M 1050W 36-72 VCC (JL758A)

Bandejas de ventilador

- Bandeja de ventilador frontal a posterior HPE Aruba Networking X371 (JL085B)
- Bandeja de ventilador de alimentación a puerto HPE Aruba Networking 630W (JL761A)
- Kit de montaje en bastidor universal HPE Aruba Networking 2/4 HU, paquete de 4 (R9S89B)

Accesorios

- Kit de montaje en bastidor universal HPE Aruba 19 de 4 soportes (R2S82A)
- Kit de montaje en bastidor universal HPE Aruba Networking 2/4 HU, paquete de 4 (R9S89B)
- Cable de PC a conmutador USB-A a RJ45 de 1.8 U HPE Aruba (R9G48B)
- Cable de red HPE Aruba USB-A a RJ45 P.N.3TX-GRY (R8Z87A)
- Cable de PC a conmutador USB-A a USB-C de red HPE Aruba (R9J93A)
- Cable de PC a conmutador USB-C a USB C de red HPE Aruba (R9J93A)
- Adaptador Bluetooth del conmutador HPE Aruba Networking, Cx/SI HE5A)
- Adaptador HPE QSFP28 a SFP28 (845970-B21)

Transceptores

- Red HPE Aruba 100 M SFP LC FX 2 km MMF XCVR (J9054D);
- Transceptor MMF HPE Aruba Networking 1G SFP LC SX de 500 m (J4858D)
- Transceptor SMF HPE Aruba Networking 1G SFP LC LX de 10 km (J4859D)
- Transceptor SMF HPE Aruba Networking 1G SFP LC LH de 70 km (J4860D)
- Transceptor CatSa HPE Aruba Networking 1G SFP RJ45 T de 100 m (J8177D)
- Transceptor TAA MMF de 500 m HPE Aruba Networking 1G SFP LC SX (JL715A)
- Transceptor SMF TAA de 10 km HPE Aruba Networking 1G SFP LC LX (JL746A)
- Transceptor TAA CatSa HPE Aruba Networking 1G SFP RJ45 T de 100 m (JL747A)
- Transceptor MMF HPE Aruba Networking 10G SFP+ LC SR 300 m (J9150D);
- Transceptor MMF HPE Aruba Networking 10G SFP+ LC LRM de 220 m (J9152D);
- Transceptor SMF HPE Aruba Networking 10G SFP+ LC LR de 10 km (J9150E);
- Transceptor SMF HPE Aruba Networking 10G SFP+ LC ER de 40 km (J9150D);
- Transceptor HPE Aruba Networking 10GBASE-T SFP+ RJ-45 CatSA de 30 m (JL563B);
- Transceptor HPE Aruba Networking 10G SFP+ LC SR 300 m MMF TAA (JL748A)
- Red HPE Aruba 10G SR SFP+ LC 400 m OM4 C-XCVR (S2P30A)
- Red HPE Aruba 10G LR SFP+ LC 10 km SMF C-XCVR (S2P31A)
- Red HPE Aruba 10G ER SFP+ LC 40 km SMF C-XCVR (S2P32A)
- Red HPE Aruba 25G SR SFP28 LC 100 m MMF C-XCVR (S2P33A)
- Red HPE Aruba 25G LR SFP28 LC 10 km SMF C-XCVR (S2P34A)
- Transceptor SMF TAA de 10 km HPE Aruba Networking 10G SFP+ LC LR (JL749A)
- Transceptor MMF HPE Aruba Networking 25G SFP28 LC SR 100 m (JL484A);
- Transceptor MMF HPE Aruba Networking 25G SFP28 LC eSR 400m (JL483A);

La capacidad de 50G se utiliza con DAC de 50G para interconexión y apilamiento VSF. Los transceptores y DAC 50G no son compatibles con los conmutadores 6000, 6100 y 6200 existentes, aunque sí son compatibles con DAC 50G a SFP56 para apilamiento VSF entre un modo de conmutador CX 6300. El apilamiento VSF no es compatible con puertos

El transceptor 8054D de 100 Mbps admite distancias de 2 km en puertos SFP+ en ESTA. Los transceptores de 10G Mbps no son compatibles con ningún puerto SFP56 en todos los modelos

J9150D XCVR compatible de fuente nueva solo en los modelos R8G91A y R8G92A

Se requiere el adaptador HPE QSFP28 a SFP28 (845970-B21) para utilizar transceptores de 1G y 25G solo cuando se usa en los modelos de conmutador R8G91A y R8G92A

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

- Transceptor SMF HPE Aruba Networking 25G SFP28 LC LR de 10 km (JL486A)
- Red HPE Aruba 25G SFP LC LR 10 km SMF TAA XCVR (S2N63A)
- Aruba 50G SFP56 LC SR 100m MMF XCVR (R0M48A)
- Transceptor MMF HPE Aruba Networking 50G eSR 300m (S0V66A)
- Transceptor SMF HPE Aruba Networking 50G LR 10 km (S0V65A)
- Transceptor SMF HPE Aruba Networking 50G ER de 40 km (S0V69A)
- Transceptor SMF HPE Aruba Networking 25G ER LC de 40 km (S0V69A)
- Transceptor HPE Aruba Networking 50G BiDi de 10 km de bajada 1330/1270 (S1C92A)
- Transceptor MMF de 100 m HPE Aruba Networking 100G SR2 MPO QSFP28 (S1C93A)
- Red HPE Aruba 4x100G DR QDD SN SMF XCVR (S3N90A)
- Transceptor HPE X142 40G QSFP+ MPO SR4 (JH231A)
- Red HPE Aruba 100G LR QSFP28 LC SMF XCVR (S3N89A)
- HPE X142 40G QSFP+ MPO eSR4 300M XCVR (JH233A)
- Transceptor MMF HPE Aruba Networking 40G QSFP+ LC BiDi de 150 m (JL308A)
- Transceptor HPE X142 40G QSFP+ LC LR4 SM (JH232A)
- Red HPE Aruba 40G QSFP+ LC ER4 40 km SMF XCVR (Q3GB2A)
- HPE 100 Gb QSFP28 XCVR bidirectional (845972-B21)
- Transceptor SMF HPE Aruba Networking 100G QSFP28 LC CWDM4 de 2 km (R0Z30A)
- Transceptor SMF HPE Aruba Networking 100G QSFP28 LC ER4 de 2 km (R9B63A)
- Transceptor HPE Aruba Networking 100G QSFP28 LC LR4 10 km SMF de 2 hilos (JL311A)
- Transceptor SMF HPE Aruba Networking 100G QSFP28 LC ERNL de 40 km (JL743A)
- Transceptor HPE Aruba Networking 50G BiDi 10 km ascendente 1270/1330 (S1C94A)
- Transceptor HPE Aruba Networking 25G BiDi de 10 km de bajada 1330/1270 (S1C96A)
- Transceptor HPE Aruba Networking 25G BiDi 10 km ascendente 1270/1330 (S1C95A)

cables

- Cable DAC HPE Aruba Networking 50G QSFP56 a SFP56 de 0,65 m (S1J07A)
- Cable DAC de 3 m HPE Aruba Networking 50G QSFP56 a SFP56 (S1J08A)
- Cable de cobre de conexión directa HPE Aruba Networking 10G SFP+ a SFP+ de 1 m (J9281D)
- Cable de cobre de conexión directa HPE Aruba Networking 10G SFP+ a SFP+ de 3 m (J9283D)
- Cable de cobre de conexión directa HPE Aruba Networking 25G SFP28 a SFP28 de 0,65 m (JL487A)
- Cable de cobre de conexión directa HPE Aruba Networking 25G SFP28 a SFP28 de 3 m (L488A)
- Cable de cobre de conexión directa HPE Aruba Networking 25G SFP28 a SFP28 de 5 m (JL489A)
- Cable DAC HPE Aruba Networking 50G SFP56 a SFP56 de 0,65 m (R0M46A)
- Cable DAC de 3 m HPE Aruba Networking 50G SFP56 a SFP56 (R0M47A)
- Cable DAC - HPE X242 40G QSFP+ a QSFP+ de 1 m (JH284A)
- Cable DAC, HPE X242 40G QSFP+ a QSFP+ de 3 m (JH235A)
- Cable DAC HPE X242 40G QSFP+ a QSFP+ de 5 m (JH236A)
- Redes HPE Aruba 40G QSFP+ a QSFP+ 7m AOC (R0Z22A)
- Redes HPE Aruba 40G QSFP+ a QSFP+ 15 m AOC (R0Z23A)
- Redes HPE Aruba 40G QSFP+ a QSFP+ 30 m AOC (R0Z24A)
- Cable DAC de 3 m HPE Aruba Networking 100G QSFP28-QSFP28 (JL307A)
- Cable de cobre de conexión directa HPE Aruba Networking 100G QSFP28 a QSFP28 de 1 m (R0Z25A)
- Cable de cobre de conexión directa HPE Aruba Networking 100G QSFP28 a QSFP28 de 3 m (JL307A)
- Cable de cobre de conexión directa HPE Aruba Networking 100G QSFP28 a QSFP28 de 5 m (R0Z26A)
- Redes HPE Aruba 100G QSFP28 a QSFP28 2 m AOC (JL856A)
- Red HPE Aruba 100G QSFP28 a QSFP28 7 m AOC (R0Z27A)
- Redes HPE Aruba 100G QSFP28 a QSFP28 15 m AOC (R0Z28A)
- Redes HPE Aruba 100G QSFP28 a QSFP28 30 m AOC (R0Z29A)

Software

- Aplicación móvil HPE Aruba Networking CX https://www.arubanetworks.com/products/networking/switches/cx-mobileapp/
- Nodo único del software de edición múltiple del conmutador de red HPE Aruba, 1 año (JL699AAE)
- Nodo único del software de edición múltiple del conmutador de red HPE Aruba, 3 años (JL699AAE)

Asociados de funciones avanzadas de HPE Aruba Networking CX

- HPE Aruba Networking CX Soft 63xx Sw Adv 10 años E-STU (S0T76AAE)
- HPE Aruba Networking CX Soft 63xx Sw Adv 1y E-STU (S0T77AAE)
- HPE Aruba Networking CX Soft 63xx Sw Adv 3 años E-STU (S0T78AAE)
- HPE Aruba Networking CX Soft 63xx Sw Adv 5 años E-STU (S0T79AAE)
- HPE Aruba Networking CX Soft 63xx Sw Adv 7 años E-STU (S0T80AAE)

¿Problemas QSFP+ y QSFP28 para uso únicamente con los modelos de conmutador 8325-32C y 9364D-GX.

Se requiere un adaptador HPE QSFP28 a SFP28 (R0Z52A) cuando se utiliza con los modelos de conmutador 9300 y 9500.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

Licencias fundacionales de HPE Aruba Networking Central

- Suscripción básica de 1 año al conmutador central de red HPE Aruba 6300/38xx E-STU (Q9Y78AAE)
- Suscripción básica de 3 años al conmutador central de red HPE Aruba 6300/38xx E-STU (Q9Y79AAE)
- Suscripción básica de 5 años al conmutador central de red HPE Aruba 6300/38xx E-STU (Q9Y80AAE)
- HPE Aruba Networking Central Switch 6300/38xx Foundational Suscripcion de 7 años E-STU (Q9Y81AAE)
- HPE Aruba Networking Central Switch 6300/38xx Suscripción básica de 10 años E-STU (R8K02AAE)
- Suscripción básica de 1 año para conmutador HPE Aruba Networking Central 63xx o 38xx E-STU (Q9Y78AAE)
- HPE Aruba Networking Central On-Premises Switch Foundational 63xx o 38xx Suscripción de 1 año E-STU (R6U83AAE)
- Suscripción básica de 3 años para conmutador HPE Aruba Networking Central local 63xx o 38xx E-STU (R6U84AAE)
- Suscripción básica de 3 años para conmutador HPE Aruba Networking Central 63xx o 38xx E-STU (Q9Y79AAE)
- HPE Aruba Networking Central On-Premises Switch Foundational 63xx o 38xx Suscripción E-STU de 5 años (R6U85AAE)
- Suscripción básica de 5 años para conmutador HPE Aruba Networking Central 63xx o 38xx E-STU (Q9Y80AAE)
- HPE Aruba Networking Central On-Premises Switch Foundational 63xx o 38xx Suscripcion E-STU de 7 años (R6U86AAE)
- Suscripción básica de 7 años para conmutador HPE Aruba Networking Central 63xx o 38xx E-STU (Q9Y81AAE)
- HPE Aruba Networking Central On-Premises Switch Foundational 63xx o 38xx Suscripcion de 10 años E-STU (R6U87AAE)
- Suscripción básica de 10 años para conmutador HPE Aruba Networking Central 63xx o 38xx E-STU (R8K02AAE)

Para obtener detalles y una lista completa de las opciones de licencia de HPE Aruba Networking Central, consulte la hoja de datos de HPE Aruba Networking Central.

Componentes de estructura de red HPE Aruba

- Switch de nivel 3 del servicio de administración de dispositivos HPE Aruba Networking Fabric Composer Suscripcion de 1 año E-STU (R8D18AAE)
- Switch de nivel 3 del servicio de administración de dispositivos HPE Aruba Networking Fabric Composer Suscripcion de 3 años E-STU (R8D19AAE)
- Switch de nivel 3 del servicio de administración de dispositivos HPE Aruba Networking Fabric Composer Suscripcion de 5 años E-STU (R8D20AAE)

Apoyo

- JL668A: 4 horas en el sitio durante 3 años (HR4C6E)
- JL669A: 4 horas en el sitio durante 3 años (HR4C7E)
- JL660A: 4 horas en el sitio 3 años (HL5Z0E)
- JL661A: 4 horas en el sitio durante 3 años (HR4B8E)
- JL662A: 4 horas en el sitio durante 3 años (HR4B9E)
- JL663A: 4 horas en el sitio durante 3 años (HR4C0E)
- JL664A: 4 horas en el sitio 3 años (HL5Z1E)
- JL665A: 4 horas en el sitio durante 3 años (HR4C1E)
- JL666A: 4 horas en el sitio durante 3 años (HR4C2E)
- JL667A: 4 horas en sitio 3 años (HR4P0E)
- JL668A: 4 horas en el sitio durante 3 años (HR4C3E)
- JL362A: 4 horas en el sitio durante 3 años (HR4A2E)

Para obtener soporte técnico (soporte de HPE Aruba Networking Central, soporte de NAE, soporte de Glcp y soporte para switches de la serie 6000 de HPE Aruba Networking), visite los servicios de soporte de HPE Aruba Networking.

Tome la decisión de compra correcta

Contáctenos

CONSORCIO EMDOC
EMDOC CONSORCIO
Santo Domingo, R.D.

Hewlett Packard Enterprise

© Copyright 2024 Hewlett Packard Enterprise Development LP. La información contenida en este documento está sujeta a cambios sin previo aviso. Las únicas garantías para los productos y servicios de Hewlett Packard Enterprise se establecen en las declaraciones de garantía expresa que acompañan a dichos productos y servicios. Nada de lo aquí contenido debe interpretarse como una garantía adicional. Hewlett Packard Enterprise no se responsabiliza de errores técnicos o de edición ni de omisiones contenidos en el presente documento.

Aruba es una marca comercial con propiedad de la compañía.

Traducción del inglés al español - www.traductorenlinea.com

Red Hat

El poder de

sombrero rojo

Linux empresarial

Flexibilidad, estabilidad y soporte
para su organización

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

Mesa de contenido

Introducción
Por qué es importante la elección de su sistema operativo
página 3

Capítulo 1
¿Qué es Red Hat? ¿Linux empresarial?
página 8

Capítulo 2
Qué ofrece una suscripción a Red Hat Enterprise Linux
página 10

Capítulo 3
Comience con Red Hat Linux empresarial
página 18

EMDOC CONSORCIO
Santo Domingo, RD



Introducción

¿Por qué la elección? de tu funcionamiento el sistema importa

Por definición, un sistema operativo (SO) es el software del sistema responsable de administrar cualquier recurso de hardware y software que su organización requiera para sus diversas operaciones.

Estructuralmente, un sistema operativo se ubica entre su hardware y los diversos servicios y aplicaciones con los que su equipo necesita interactuar para realizar su trabajo de manera efectiva y eficiente.

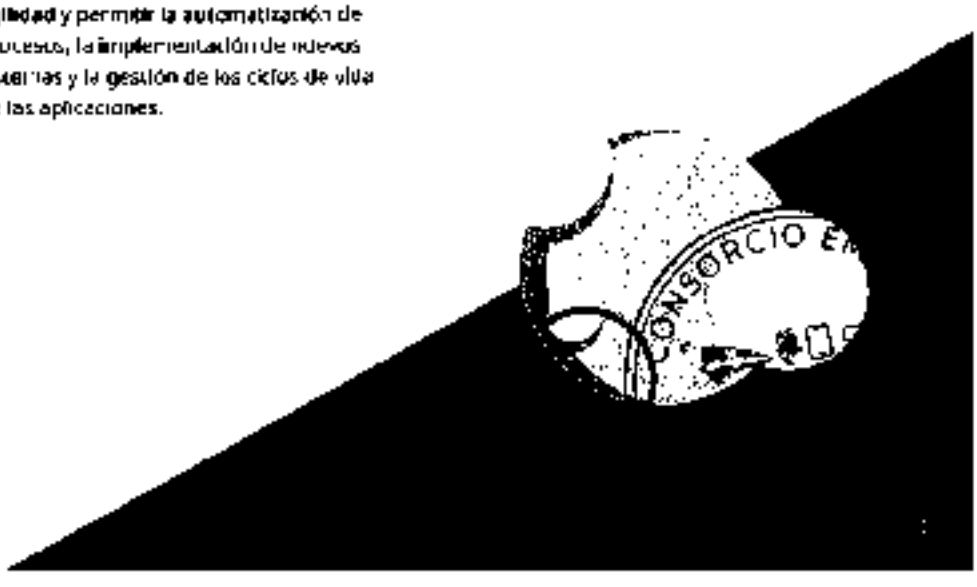
También se confía en su sistema operativo para controlar la variedad de tareas que requieren sus aplicaciones, como administración de energía, administración del rendimiento, subprocesamiento regional y seguridad. Esto garantiza que su red de aplicaciones y servicios pueda funcionar de manera eficiente y en armonía, sin importar desde dónde esté operando el usuario.

Unifique su infraestructura de TI con el sistema operativo adecuado

Los líderes empresariales de todos los sectores buscan un entorno de TI que pueda proporcionar **flexibilidad, adaptabilidad, resiliencia y manejabilidad.**

La capacidad de proporcionar estos factores es un reflejo directo de su entorno operativo general y lo más importante, su sistema operativo.

Como base que facilita las capacidades más cruciales de su organización, es esencial que su sistema operativo sea capaz de proporcionar estandarización en todo su sistema operativo entorno, incluidos entornos de nube física, virtual, privada y pública, y el borde de una red, para facilitar la innovación y la agilidad y permitir la automatización de procesos, la implementación de nuevos sistemas y la gestión de los ciclos de vida de las aplicaciones.



¿Qué es un sistema operativo de código abierto?

Al buscar el sistema operativo adecuado para su organización y sus necesidades específicas, es mejor comprender primero los dos tipos distintos, en qué se diferencian entre sí y los beneficios que ofrece cada uno.

SO de código cerrado
Un sistema operativo de código cerrado, también conocido como sistema operativo propietario, como Windows de Microsoft o macOS de Apple, se construye con un código fuente que se mantiene privado e inaccesible para terceros y, por lo tanto, solo puede ser personalizado por el propietario del código o mediante herramientas de socios aprobados.

SO de código abierto
Un excelente ejemplo de un sistema operativo de código abierto es Linux®, que brinda a todos los usuarios la capacidad de modificar el código fuente para adaptarlo a las necesidades de su organización, y cuenta con una comunidad completa de desarrolladores que crean nuevas herramientas y soluciones que están disponibles para cualquier usuario de Linux que desee aprovecharlas.

Aumento previsto en el uso de software empresarial de código abierto[1]



Si bien ambos tipos de sistemas operativos son utilizados ampliamente por empresas de todo el mundo, el software de código abierto en su conjunto ha ido ganando popularidad en los últimos años, mientras que el software propietario pierde popularidad cada año.[1]

El informe sobre el estado del código abierto empresarial 2022 de Red Hat predice que en los próximos dos años, el uso de software empresarial por parte de las empresas subirá del 85% al 87%, mientras que el se prevé que el uso de código abierto basado en la comunidad aumente del 21 % al 24 %.[1]

Con el software de código abierto ganando popularidad, uno de los desarrollos más notables ha sido el surgimiento del software de código abierto empresarial, que viene con su propio conjunto de ventajas en comparación con el código abierto basado en la comunidad, incluidas mejoras notables en seguridad y confiabilidad.

A medida que más proveedores de software empresarial comienzan a reclamar su presencia en la comunidad de código abierto con sus propias soluciones de código abierto, se predice que el software de código abierto empresarial verá un aumento en su uso del 29% al 34% en los próximos 2 años.[1]

---

[1] Informe Redhat, "El estado del código abierto empresarial: un informe de Red Hat," 22 de febrero de 2022.

CONSORCIO EMDOC
EMDOC
Santo Dom

Beneficios de un sistema operativo de código abierto

Un sistema operativo de código abierto produce una lista de beneficios que muchas organizaciones necesitan para sus aplicaciones y que a menudo son difíciles de lograr con un sistema operativo de código cerrado: rentabilidad, confiabilidad y flexibilidad.

Eficiencia de costo

Debido a que los sistemas comerciales de código abierto suelen ser menos costosos que sus homólogos de código cerrado y, en algunos casos, incluso sus creadores los proporcionan de forma totalmente gratuita, un sistema operativo de código abierto puede proporcionar una mayor rentabilidad que sus homólogos de código cerrado.

Fiabilidad

Debido a que el código fuente de un sistema operativo de código abierto está disponible públicamente, miles de desarrolladores de todo el mundo lo revisan y cualquier error o vulnerabilidad existente en el código fuente se encuentra y corrige rápidamente.

Flexibilidad

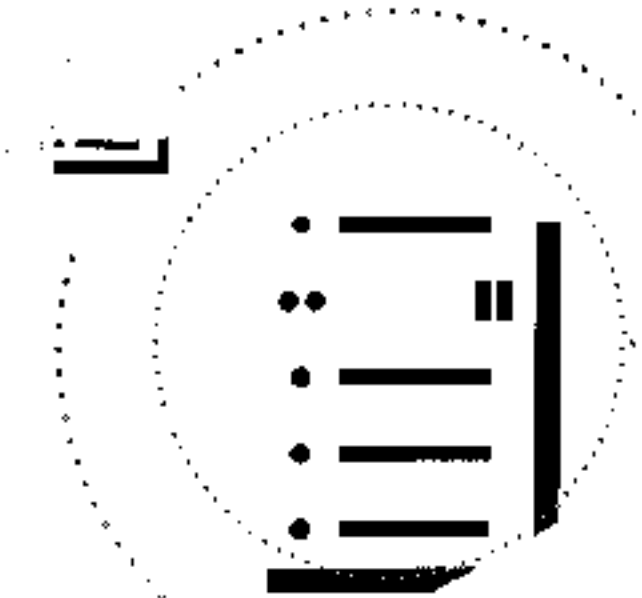
Como sistema operativo con código fuente personalizable y disponible públicamente, con las habilidades adecuadas, su sistema operativo puede ser y hacer lo que su organización necesita que haga. Entendido un nivel de flexibilidad que no es posible con un sistema operativo de código cerrado.

A pesar de estas importantes ventajas, el software de código abierto basado en la comunidad todavía tiene ciertas desventajas.

Lo más notable es el riesgo de utilizar software de origen comunitario en lugar de una solución desarrollada en colaboración con la comunidad y luego mejorada en materia de seguridad, cumplimiento y certificaciones de terceros por parte de un desarrollador y proveedor de software empresarial.

Afortunadamente para las organizaciones que buscan aprovechar las ventajas del software de código abierto, estas desventajas se abordan directamente en el mercado empresarial emergente de código abierto.

Las soluciones empresariales de código abierto se crean con software de código abierto que ha sido reforzado por un proveedor de software empresarial mediante pruebas y ajustes de rendimiento, y luego respaldado por soporte y servicios empresariales, que a menudo incluyen actualizaciones y controles de seguridad proactivos.





Ventajas de las soluciones empresariales de código abierto

El software empresarial de código abierto se ha vuelto tan esencial para las prácticas de TI en el espacio empresarial que el 95 % de los líderes de TI dicen que el código abierto empresarial es importante para la infraestructura empresarial general de su organización y el 60 % de los líderes de TI esperan aumentar su uso del software empresarial de código abierto para tecnologías emergentes.[1]

Pero, ¿cuáles son las mayores ventajas que estas organizaciones están obteniendo con las soluciones empresariales de código abierto?

Entre las ventajas más notables del software empresarial de código abierto identificadas por los líderes de TI se encuentran un software de mayor calidad y una mejor seguridad. Y si bien la falta de soporte a menudo se menciona como una de las mayores dudas para las organizaciones que consideran adoptar el código abierto empresarial, casi siempre vienen con amplios servicios de soporte.

Software de mayor calidad El mayor nivel de calidad se logra a través de pruebas exhaustivas y ajustes de rendimiento que realiza el proveedor de software de código abierto empresarial antes de lanzar la solución al mercado, lo que reduce el riesgo de problemas desconocidos o inesperados que a veces pueden surgir con el software de origen comunitario.

Seguridad
El 89 % de los líderes de TI afirma que la seguridad de las soluciones empresariales de código abierto es tan buena o mejor que la seguridad del software propietario, siendo las razones más comunes la disponibilidad de parches de seguridad que están bien documentados y pueden escanearse, la pronta disponibilidad de vulnerabilidades parches de los proveedores, el hecho de que más personas han puesto sus ojos en el código y la capacidad de que sus propios equipos trabajen el código.[1]

Apoyo
Las soluciones empresariales de código abierto casi siempre vienen equipadas con amplias herramientas y recursos de soporte, con frecuencia incluye soporte telefónico y en línea para incidentes, bases de datos y portales de soporte, y herramientas y actualizaciones de seguridad automatizadas. Hasta este punto, uno de los principales razones enumeradas por los líderes de TI con respecto a por qué prefieren proveedores de software empresarial de código abierto fue su ubicación para soporte técnico.[1]

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo R.D.



Por qué Linux es el sistema operativo de código abierto preferido

Lo primero es lo primero: ¿qué es Linux?

Linux es un sistema operativo que comúnmente se entrega como parte de un paquete generado más grande por parte de varios distribuidores, y viene con una variedad de capacidades y herramientas incluidas.

Como el sistema operativo de código abierto más popular del mundo[1] y el sistema operativo más popular en general,[2] Linux se ha desarrollado durante mucho tiempo al servicio de las empresas que utilizan prácticas de TI modernas e innovadoras, especialmente para aquellas que se centran en el desarrollo de software.

Investigaciones recientes muestran que Linux es el segundo sistema operativo de PC más popular para el desarrollo de software. El 47 % de los desarrolladores encuestados citan Linux como distribución del sistema operativo de su PC.[3]

Desde una perspectiva de la nube, el estudio de mercado de Linux 2021 realizado por Management Insight Technologies, un estudio de mercado interno realizado en nombre de Red Hat, encontró que el 49 % de los encuestados tiene instancias de Linux en la nube, el 28 % en la nube pública y el 21 % en la nube privada.[4]

Su adopción generalizada en industrias y tecnologías emergentes continúa creciendo y, tras décadas de pruebas, Linux ha demostrado ser la plataforma ideal para resolver las prácticas de TI innovadoras que se necesitan hoy.

Su popularidad entre las empresas modernas se acopla más comúnmente con la flexibilidad y compatibilidad que proporciona.



Más popular

SO[2] de código abierto



Más popular

SO en general

Flexibilidad

Esta flexibilidad se logra en gran parte debido a que no es necesario instalar una suite completa, sino solo los componentes que necesita, permitiendo que su organización opere sin herramientas o componentes innecesarios.

Compatibilidad

Linux no solo puede ejecutar cualquiera y todos los formatos de archivos, sino que también tiene el poder de facilitar el desarrollo y la operación de las cargas de trabajo más críticas de su organización en entornos informáticos de todo tipo y admitir una amplia gama de casos de uso, sistemas de destino y dispositivos.

Obtenga más información sobre por qué Linux es el sistema operativo

[redacted]

En este libro electrónico exploramos la importancia de un sistema operativo como Linux y, específicamente, los beneficios que la plataforma Red Hat® Enterprise Linux puede aportar a su organización.

---

[1] "Cuota de mercado global de sistemas operativos (diciembre 2012-2022, por mes)." Statista. 29 de agosto de 2022. "Cuota de mercado de sistemas operativos de PC de enero de 2013-2022, por mes." Statista. 29 de julio de 2022. "Distribución de registros de usuarios de sistemas operativos de PC de enero de 2018 a 2021." Statista. 29 de julio de 2022. Libro electrónico de Red Hat.

[2] "Estado de Linux en la nube pública y creación anual." 9 de agosto de 2021.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

Capítulo 1:

¿Qué es Red Hat? ¿Linux empresarial?

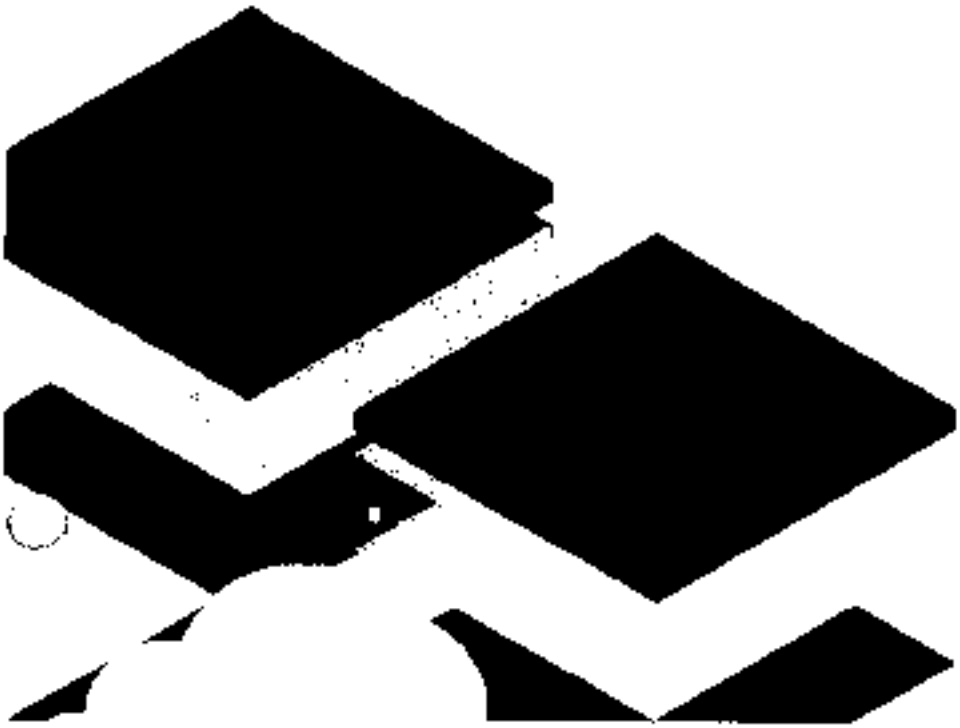
Como una de las plataformas Linux empresariales más populares del mundo[1], Red Hat Enterprise Linux está certificado para su uso con clientes de entornos de nube y con miles de proveedores de software y hardware.

Además de la compatibilidad que puede brindar a organizaciones de todos los tamaños que buscan obtener una verdadera ganancia de valor a sus cargas de software, también brinda las capacidades innovadoras que necesitan las organizaciones actuales con su acceso a una extensa red de herramientas y el soporte necesario para administrar cualquier complejidad añadidos con su soporte líder en el sector las 24 horas.

Dado que las distribuciones de Linux están disponibles a través de todos los principales proveedores de nube pública, incluidos Microsoft Azure, Amazon Web Services (AWS), Google Cloud, IBM Cloud y Alibaba Cloud, con diferentes características, integraciones, soportes y asociaciones, es vital que elija la distribución adecuada para su organización y sus necesidades.

Teniendo esto en cuenta, ¿cómo aborda Red Hat Enterprise Linux los desafíos más comunes que enfrentan las organizaciones de todos los tamaños que operan prácticas de TI modernas y buscan optimizar sus recursos con soluciones rentables?

1 [redacted] noviembre de 2022.





Afrontar los desafíos modernos con una plataforma de sistema operativo moderna

Uno de los mayores desafíos que enfrentan las organizaciones es encontrar un sistema operativo que proporcione la coherencia y eficiencia necesarias para gestionar las complejidades ahondadas de las prácticas de TI modernas en todo su entorno de TI.

Al brindar coherencia en su entorno de TI y sus diversas infraestructuras (incluidos entornos de nube física, virtual, privada y pública, e implementaciones de borde), Red Hat Enterprise Linux lo ayuda a administrar sus aplicaciones, cargas de trabajo y servicios con las mismas herramientas, sin importar el ubicación.

Otros desafíos comunes que enfrentan las organizaciones que aplican prácticas de TI modernas incluyen la necesidad de crear un entorno de TI más seguro y confiable y la necesidad de acelerar el tiempo de generación de valor en cargas de trabajo comerciales críticas.

Estos desafíos se abordan directamente mediante las herramientas integradas y el soporte de una suscripción a Red Hat Enterprise Linux.

Entre muchos otros beneficios, los clientes existentes que utilizan Red Hat Enterprise Linux han logrado una serie de mejoras operativas en comparación con las soluciones de código abierto gratuitas, según una investigación independiente de IDC.[1]

Entorno de TI confiable y centrado en la seguridad

72% menos imprevistos
Tasa del tiempo

Consistencia y eficiencia

32% TI más eficiente
equipos de infraestructura.

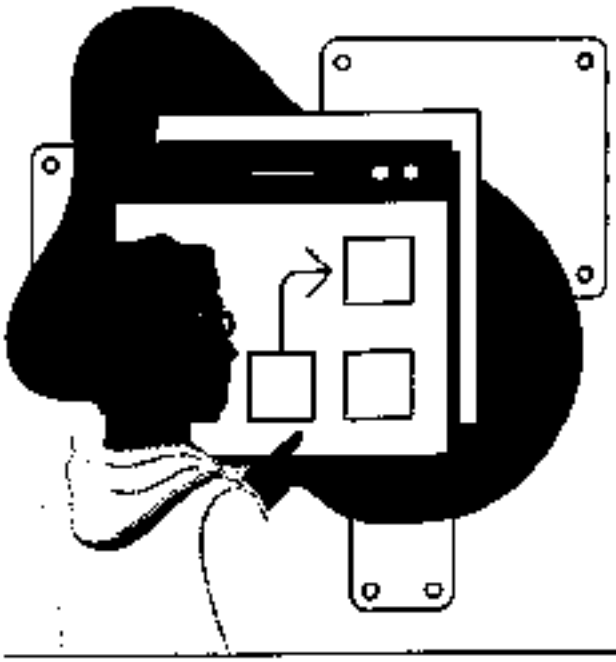
Menores costos operativos

$172K ahorro en costos de infraestructura de nube por organización por año.

Acelere el tiempo de obtención de valor

23% Ciclo de vida de desarrollo más rápido
para nuevas aplicaciones.

20% más productivo
equipos de desarrollo.



Descubra por qué el uso de Red Hat Enterprise Linux para respaldar las actividades comerciales proporcionará a los clientes un impulso de 1,7 billones de dólares en mayores ingresos y optimización de recursos.

[redacted]

[1] Estudio de banco de IDC, patrocinado por Red Hat, "[redacted]" Documento #US50103323, marzo de 2023

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

Capítulo 2:

Qué ofrece una suscripción a Red Hat Enterprise Linux

A medida que su organización busca afrontar el desafío de encontrar el sistema operativo adecuado debe saber que tiene que proporcione la coherencia y eficiencia necesarias para gestionar las cargas de TI modernas. Es importante tener en cuenta que, además de los amplios beneficios que puede proporcionar un entorno operativo Linux, también requiere las herramientas y el soporte adecuados para garantizar su gestión adecuada.

Con Red Hat Enterprise Linux, se le proporcionarán esas herramientas y soporte como parte de su suscripción, lo que le permitirá a su equipo técnico la libertad de continuar innovando sin la carga de administrar esas necesidades.

Con Red Hat Enterprise Linux, usted tiene:

- Flexibilidad y control sobre todo su entorno de TI
- Acceso a las últimas innovaciones de Linux.
- Implementaciones admitidas en cualquier lugar.
- Funciones de seguridad y soporte de nivel empresarial
- Acceso a las últimas innovaciones en el ecosistema de socios certificados de Red Hat.
- Estabilidad de las tecnologías emergentes.

Obtenga más información sobre lo que incluye una suscripción a Red Hat Enterprise Linux en esta guía detallada.

[redacted]

CONSORCIO EMDOC
EMDOC
Santo Domingo

Flexibilidad y control en todos los entornos, versiones y costos de TI

Cada organización tiene necesidades y requisitos únicos que requieren la capacidad de adaptar un entorno de TI para satisfacer esas necesidades, sin exceder las restricciones de costos y soporte.

Una suscripción a Red Hat Enterprise Linux proporciona el nivel necesario de flexibilidad a través de:



Portabilidad entre entornos de TI. Debido a que su suscripción no está vinculada a ninguna ubicación de instalación, proveedor de nube o hardware específico, puede aplicar sus suscripciones a una amplia selección de sistemas físicos, virtuales, de nube o de borde y moverlos según sea necesario para satisfacer las necesidades y requisitos únicos de su organización.

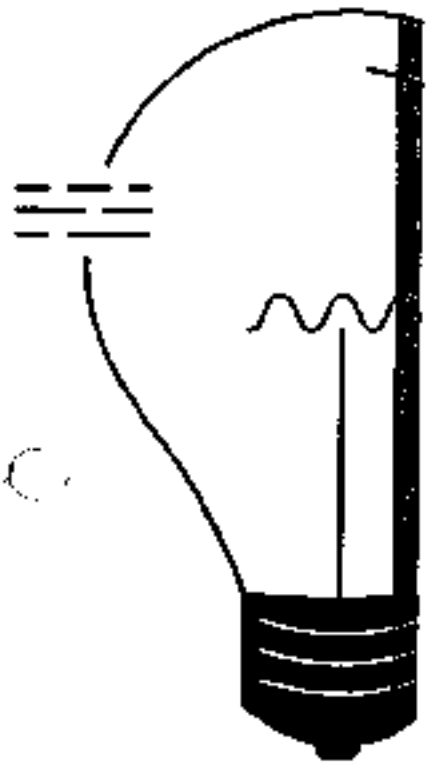
Soporte para todas las versiones mantenidas. Con acceso y soporte para cada versión mantenida activamente de Red Hat Enterprise Linux, su suscripción le permite a su organización administrar actualizaciones según un cronograma que satisfaga sus necesidades únicas, al tiempo que garantiza soporte garantizado en el futuro con estandarización en las principales versiones para hasta 10 años.

Mayor control y costes flexibles

Una suscripción a Red Hat Enterprise Linux le brinda un control más inmediato sobre sus gastos de TI al trasladarlos de gastos de capital (CapEx) a gastos operativos (OpEx), al tiempo que proporciona un mayor nivel de control sobre el alcance de esos costos con una gama de niveles personalizables de soporte para satisfacer las necesidades de su organización con un presupuesto que tenga sentido para usted. Red Hat también trabaja con proveedores de nube para ofrecer opciones de compra convenientes para clientes conjuntos. Puede traer su propia suscripción, pagar sobre la marcha (bajo demanda), utilizar el gasto comprometido del proveedor de la nube e incluso trabajar directamente con Red Hat para crear un plan personalizado adaptado a sus necesidades específicos.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

Obtenga acceso a las últimas innovaciones de Linux



Con una suscripción a Red Hat Enterprise Linux, obtiene acceso a las últimas innovaciones de Linux listas para la empresa disponibles, todas las cuales están certificadas para su uso con el amplio portafolio de software, automatización y tecnologías de administración de Red Hat, incluidas Red Hat Smart Management y Red Hat Ansible® Automation Plataforma y Red Hat OpenShift®.

Pero una suscripción a Red Hat Enterprise Linux es más que acceso a productos innovadores.

Como base sobre la que se construye todo el portafolio de Red Hat, se incluye una suscripción a Red Hat Enterprise Linux para brindar niveles de soporte específicos, actualizaciones y mantenimiento del ciclo de vida, visibilidad de la hoja de ruta de Red Hat Enterprise Linux y herramientas para actualizar, parchear y automatizar y analizar su entorno, todo lo cual se describirá con mayor detalle en las siguientes secciones.



CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

Implementaciones admitidas en cualquier lugar, desde el centro de datos hasta el borde

La variedad de casos de uso que se pueden admitir a través del ecosistema de socios certificados de Red Hat se vuelve cada vez más importante a medida que las empresas continúan diversificando dónde implementan sus cargas de trabajo, el uso de la nube continúa aumentando cada año y las implementaciones de borde se convierten en una necesidad para las empresas que necesitan tener recursos informáticos más cerca de la fuente.

En Red Hat, entendemos que organizaciones como la suya tienen requisitos únicos cuando se trata de lograr sus estrategias de nube en su patrimonio de TI. Es por eso que Red Hat Enterprise Linux ofrece la máxima flexibilidad: brinda un entorno consistente y estable que lo acompaña dondequiera que se encuentre en su viaje a la nube.

Red Hat Enterprise Linux está certificado para su uso con clientes de socios de nube, incluidos Microsoft Azure, AWS, Google Cloud Platform, IBM Cloud y Alibaba Cloud. Con capacidades diseñadas conjuntamente y optimizadas para el uso de la nube, Red Hat ofrece una experiencia consistente pero flexible en entornos públicos, privados, híbridos y multinube.

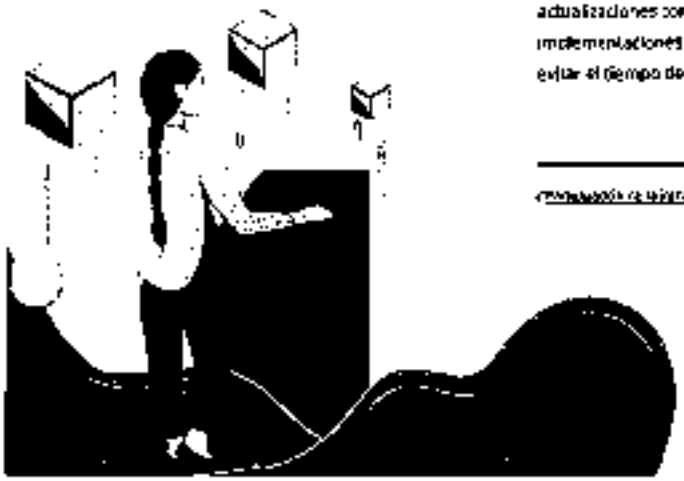
A medida que las implementaciones perimetrales siguen ganando popularidad, echemos un vistazo más de cerca a cómo una suscripción a Red Hat Enterprise Linux brinda soporte a su empresa.

Llevando su empresa al límite

A medida que más empresas comienzan a ejecutar implementaciones en el borde, con predicciones que muestran que para 2022 más de la mitad de la nueva infraestructura de TI empresarial se implementará en el borde en lugar de centros de datos centralizados[1], el soporte para implementaciones perimetrales es cada vez más importante.

Con Red Hat Enterprise Linux, obtiene la base ideal para implementaciones de borde en entornos de infraestructura pequeña, con la coherencia entre infraestructuras, la portabilidad de cargas de trabajo y las operaciones optimizadas necesarias para facilitar el traslado de cargas de trabajo tradicionales y en contenedores desde su centro de datos a sus ubicaciones de borde.

Además, Red Hat Enterprise Linux proporciona imágenes de sistema operativo optimizadas personalizadas para admitir una amplia gama de cargas de trabajo que se ejecutan en cualquier tipo de sitios remotos, las actualizaciones confiables de imágenes y sistemas necesarias para limitar las interrupciones operativas en implementaciones con ancho de banda limitado o baja conectividad, reversiones para ayudarlo a evitar el tiempo de inactividad al administrar una gran cantidad de dispositivos y ubicaciones.



[1] "Predicción de tendencias empresariales de TI para 2020: Edge Infrastructure", Gartner, 29 de noviembre de 2019.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

Soporte y seguridad de nivel empresarial que van más allá de las mejores prácticas

En primer lugar, su suscripción a Red Hat Enterprise Linux le brinda acceso a soporte telefónico y en línea en caso de incidentes para brindar tranquilidad a su organización mientras opera en los complejos entornos de TI necesarios para las prácticas de TI modernas e innovadoras.

Para las organizaciones que requieren más que soporte y mejores prácticas recomendadas, pueden acceder al portal de clientes de Red Hat que ofrece información sobre las vulnerabilidades de seguridad actuales y los pasos críticos que se deben tomar para mitigar su impacto, así como una extensa base de datos de arquitectura de referencia, documentación, videos y debates colaborativos con expertos de Red Hat.



Algunas otras formas en que Red Hat Enterprise Linux brinda el soporte y la seguridad que necesita para ejecutar un entorno de TI eficiente, confiable y centrado en la seguridad en su organización.



Seguridad multinivel y cumplimiento simplificado

A través de su suscripción a Red Hat Enterprise Linux, puede brindarle a su organización protección multinivel contra amenazas, herramientas de seguridad flexibles y formas más sencillas de mantener el cumplimiento.

Esto se logra a través de herramientas de escaneo y remediación y acceso continuo a nuevos recursos para ayudarlo a garantizar el cumplimiento continuo de su organización, así como herramientas de seguridad automatizadas, actualizaciones periódicas y lanzamientos de parches, e inteligencia y experiencia en seguridad accesibles para mejorar el enfoque de su organización en la seguridad.

Y, por último, con la certificación de estrictos estándares de seguridad, puede permitir que su organización utilice Red Hat Enterprise Linux en todas y cada una de las industrias y situaciones sin comprometer la seguridad o los requisitos de cumplimiento.

Análisis integrado con corrección, gestión y automatización.

Red Hat Insights, un software como servicio que viene incluido en todas las suscripciones activas de Red Hat Enterprise Linux, recopila de forma proactiva análisis en todo su entorno, lo que le permite confiar en él para identificar amenazas de seguridad, cuellos de botella y configuraciones erróneas que podrían afectar directamente alterar la disponibilidad, el rendimiento y la estabilidad de cualquier aspecto de su entorno de TI.

Y con la capacidad de Red Hat Enterprise Linux para integrarse con otras herramientas de automatización y administración de Red Hat, como Red Hat Satellite y Red Hat Ansible Automation Platform, su organización puede lograr eficiencia en todos los aspectos de las operaciones.



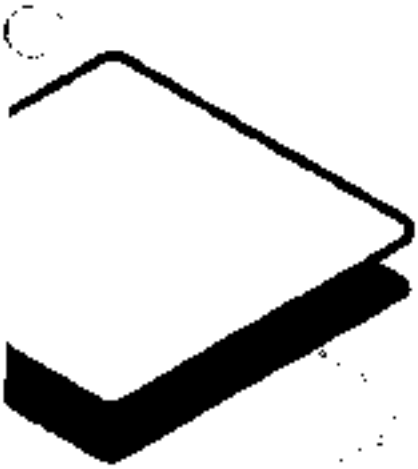
CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.



Optimiza tus recursos

Red Hat Insights Resource Optimization proporciona un servicio único y consistente para actualizar los productos de Red Hat que se ejecutan en la nube pública, la nube híbrida y en instalaciones, analizando plataformas y aplicaciones para predecir problemas, recomendar acciones y realizar el seguimiento de los costos para que las cargas de trabajo se puedan administrar con mayor rapidez y flexibilidad.

Está diseñado para ayudar a los clientes de Red Hat Enterprise Linux a obtener información y control sobre su gasto en la nube pública recomendando el tamaño correcto del sistema de nube pública para un caso de uso particular.



Un ecosistema de socios certificados para todos los entornos de TI

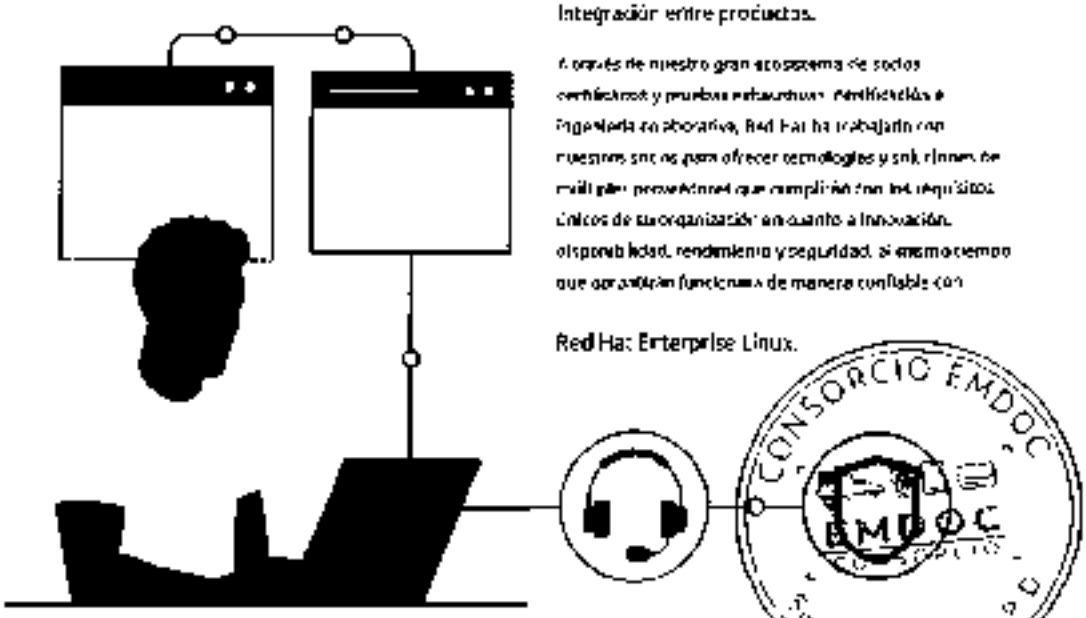
Red Hat ha fomentado asociaciones estrechas con todos los proveedores de hardware, software y nube líderes en la industria. Con su suscripción a Red Hat Enterprise Linux, esas asociaciones le brindan la flexibilidad de elección que necesita para garantizar la innovación y la estabilidad dentro de su entorno de TI.

Ese ecosistema de socios certificados le proporciona a su organización una amplia gama de opciones en arquitecturas y soluciones a través de una cadena de suministro de software confiable, todas las cuales están certificadas para su uso con productos Red Hat y cuentan con interoperabilidad en todo su entorno de TI, lo que le permite construir una plataforma de TI ambiente con

Integración entre productos.

A través de nuestro gran ecosistema de socios certificados y pruebas exhaustivas certificadas e ingeniería colaborativa, Red Hat ha trabajado con nuestros socios para ofrecer tecnologías y soluciones de múltiples proveedores que cumplirán con los requisitos únicos de su organización en cuanto a innovación, disponibilidad, rendimiento y seguridad, al mismo tiempo que garantizan funciones de manera confiable con

Red Hat Enterprise Linux.



CONSORCIO EMDOC
EMDOC
Santo Domingo, D.

Planifique su hoja de ruta de TI con visibilidad de las tecnologías emergentes

Muchas organizaciones con visión de futuro ponen gran énfasis en mantener la visibilidad de las tecnologías emergentes y cómo pueden afectar sus operaciones.

Por lo general, esto incluye centrarse en utilizar esa visibilidad para priorizar cuáles de esas tecnologías servirían mejor a sus necesidades organizativas y diseñar una hoja de ruta de TI que planifique la incorporación de esas tecnologías.

Con una suscripción a Red Hat Enterprise Linux, obtiene visibilidad avanzada gracias a los esfuerzos proactivos de Red Hat para identificar tecnologías emergentes importantes para sus clientes y avisarlos sobre cualquier característica nueva que esté disponible próximamente.

Esto permite a los clientes de Red Hat Enterprise Linux planificar con precisión su hoja de ruta de TI por adelantado mientras esperan que Red Hat desarrolle esas tecnologías en aplicaciones libres para la empresa que satisfagan las necesidades futuras de TI.

Además de obtener este nivel de visibilidad, puede tener una influencia directa en el desarrollo de cualquier nueva aplicación o característica que surja en el horizonte.

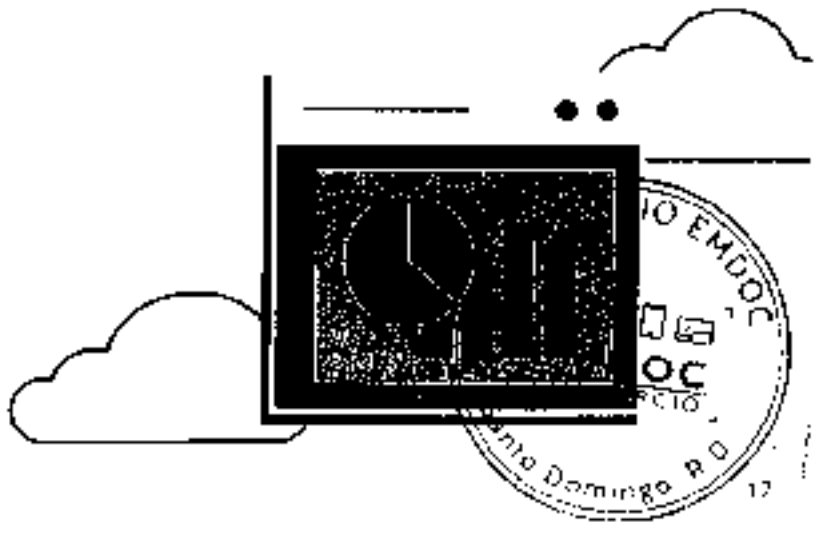
La naturaleza colaborativa de la relación de Red Hat con sus clientes incluye el mandato de conocer, evaluar e incorporar las necesidades de esos clientes en el desarrollo futuro.

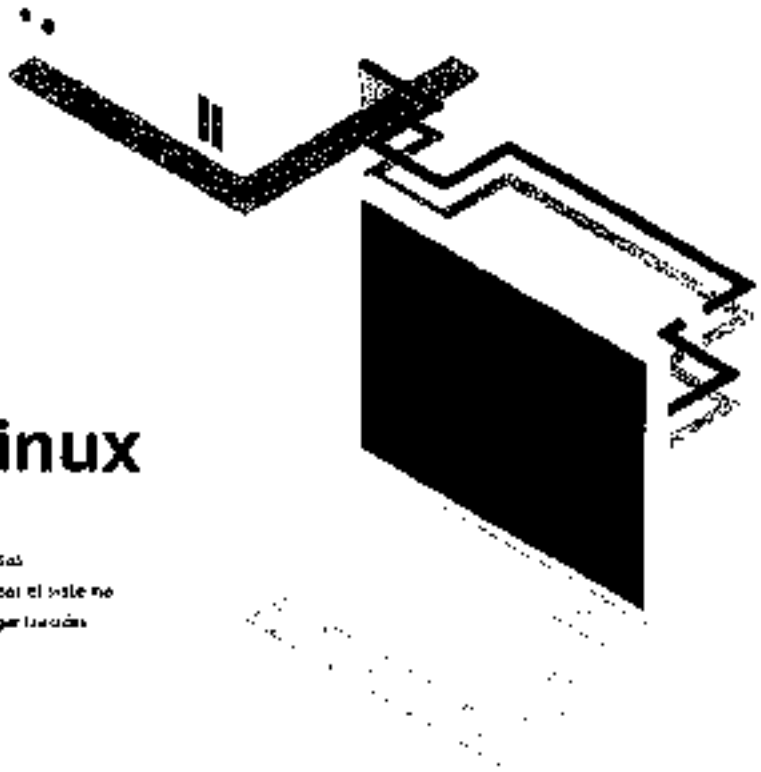
Esto le permite planificar aplicaciones o funciones futuras e incluso tener una influencia directa en cómo se desarrollan.

Debido a la extensión de la red de clientes de Red Hat, su organización también puede beneficiarse de las mejoras intersectoriales de los productos Red Hat que se desarrollaron en colaboración con otros clientes.

Todo esto permitirá que su organización se mantenga a la vanguardia de la curva tecnológica a medida que las empresas convierten más cargas de trabajo y procesos cada año.

Aprenda cómo obtener valor y beneficios en siete áreas operativas clave con Red Hat Enterprise Linux.





Capítulo 3:

Empezar con Red Hat Enterprise Linux

A través de su suscripción a Red Hat Enterprise Linux, obtendrá acceso a las diversas herramientas, funciones de seguridad y recursos de soporte que necesita para crear el sistema operativo consistente, confiable, inteligente y con foco en la seguridad que su organización necesita para operar prácticas de TI modernas.

Esto incluye:



Flexibilidad y control sobre todo su entorno de TI.



Acceso a la última versión de Linux e innovaciones.



Implementaciones admitidas en [illegible]



Soporte de nivel empresarial y [illegible] de seguridad.



Acceso a la innovación de Red Hat, ecosistema de socios certificados



[illegible] tecnologías.



¿Está interesado en aprender más sobre Red Hat Enterprise Linux y las poderosas capacidades y beneficios que puede brindarle a su organización? Por favor visite redhat.com/rhel.

¿Listo para comenzar?

Pruebe un Prueba de 60 días de Red Hat Enterprise Linux hoy.

Copyright © 2023 Red Hat, Inc. Red Hat, el logotipo de Red Hat, Ansible y OpenShift son marcas comerciales o marcas comerciales registradas de Red Hat, Inc. o sus subsidiarias en los Estados Unidos y otros países. Linux® es la marca registrada de Linus Torvalds en EE. UU. y otros países.

CONSORCIO EMDOC
EMDOC
Santo Domingo, R.D.

Obtenga una ventaja competitiva gracias a su estrategia de Linux

Una base para simplificar la infraestructura de nube híbrida

Red Hat

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

Resumen para ejecutivos 3

Capítulo 1

Saque el máximo partido a la plataforma Linux

Razones para elegir Linux 5

Importancia de la distribución de Linux 5

Consejos para elegir la plataforma Linux adecuada 6

Aumento de la agilidad con un enfoque de nube híbrida y el uso de contenedores 7

Capítulo 2

Ventajas de Linux

Ayuda para la estandarización en todos sus entornos 8

Aceleración de la innovación dondequiera que se produzca 8

Una base estable y centrada en la seguridad 9

Operaciones seguras 9

Capítulo 3

El enfoque de Red Hat

Más que un sistema operativo: una base de desarrollo 10

Seis ventajas de utilizar Red Hat Enterprise Linux 11

Conozca las ventajas que ofrece Red Hat Enterprise Linux 16

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo RD

Resumen para ejecutivos

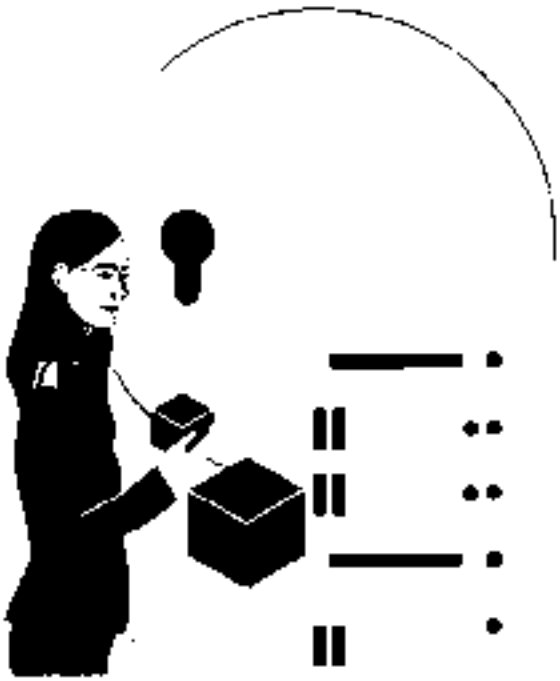
Las empresas que operan en todo el mundo, y en casi todos los sectores, reconocen las ventajas de utilizar Linux® para alcanzar sus objetivos de innovación en TI.

Linux, uno de los sistemas operativos (SO) de servidor más conocidos, ofrece a las empresas una plataforma idónea para adoptar las últimas tecnologías. Se convirtió en la solución estándar para desarrollar y ejecutar las cargas de trabajo más importantes, confiables y de gran disponibilidad, ya sea en el centro de datos, en un entorno de nube o en el extremo de la red.

En la era del cloud computing, la importancia del sistema operativo empresarial se está redefiniendo. A medida que las cargas de trabajo se trasladan progresivamente a la nube y a los entornos híbridos, el tipo de sistema operativo que elija puede parecer una cuestión secundaria; sin embargo, la calidad de la infraestructura de TI depende de su base. Esa base debe constituir la estrategia fundamental de la empresa, en la que el sistema operativo elegido debe desempeñar un papel central.



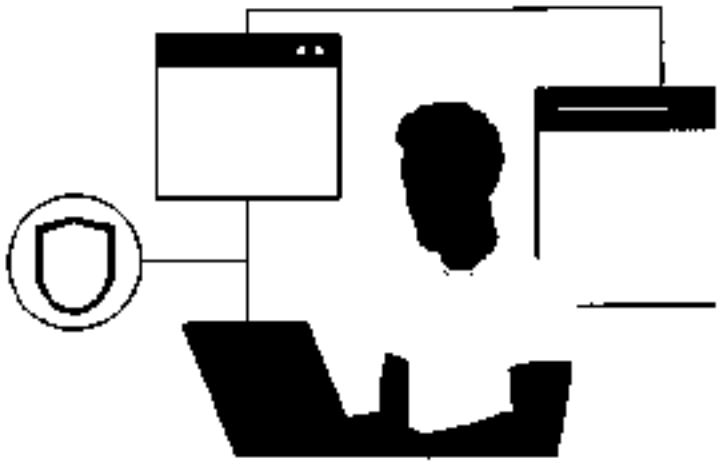
Con el auge del edge computing, las cargas de trabajo se trasladan incluso más allá de los centros de datos centrales y los entornos de nube y, por tanto, ya no se elige solo entre dos sistemas operativos. Las características del sistema abierto Linux, y su presencia en los principales proveedores de servicios en la nube, como Microsoft Azure, Amazon Web Services (AWS) o Google Cloud Platform, ofrecen a las empresas la flexibilidad de elegir entre una amplia variedad de distribuciones de Linux, ya sean versiones gratuitas o de pago.



CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

La elección de la plataforma Linux adecuada es fundamental a la hora de gestionar los desafíos que suponen las TI cada vez más complejas y competitivas. No obstante, ante tanta flexibilidad y opciones, cabe plantearse el modo en que su empresa puede tomar la decisión correcta.

En este ebook, se analizan algunos factores que hay que tener en cuenta a la hora de elegir una distribución Linux o una combinación de distribuciones y los motivos por los que esa decisión es fundamental para la innovación, el rendimiento, la eficiencia y mucho más.



Linux: ¿versiones gratuitas o de pago?

Los proveedores de servicios de nube tratan de fomentar la adopción de las distribuciones de Linux que no suponen costo alguno, y muchos de ellos utilizan las suyas propias para destacarse. La elección del sistema operativo adecuado para las necesidades de su empresa requiere la elaboración de una estrategia vanguardista. Para ello, las empresas deben tener en cuenta los desafíos a los que se enfrentan en los entornos híbridos y multicloud, así como las soluciones de TI modernas que desean implementar, tales como la virtualización, el edge computing, la organización en contenedores y el desarrollo en la nube.

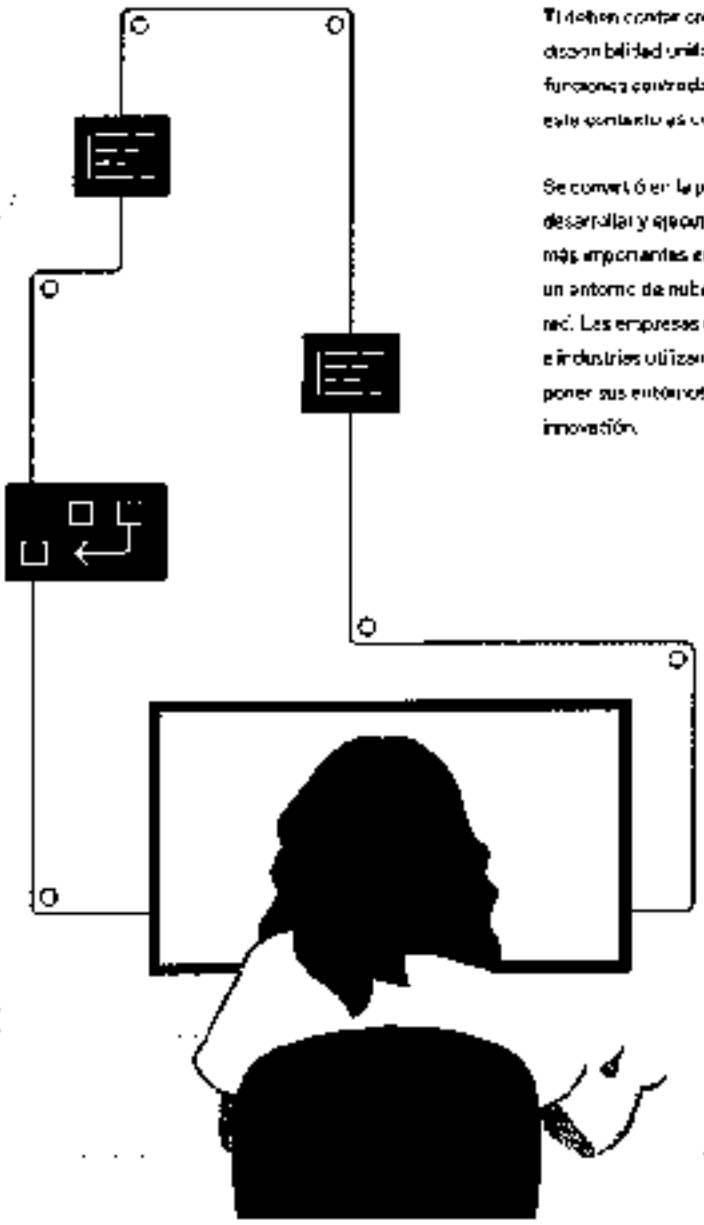
Si bien para algunos la opción de Linux más adecuada es aquella gratuita y de autogestión, una distribución de pago puede ayudar a que la empresa sea más innovadora, competitiva y eficaz. Según IDC, los gastos operativos (OpEx) asociados al mantenimiento del software open source gratuito son más altos que los que corresponden al software open source basado en suscripciones de Red Hat®

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

'White paper de IDC, patrocinado por Red Hat: 'El valor empresarial de las soluciones de Red Hat en contraste con las alternativas gratuitas'. Doc. n.º US47607721, Mayo de 2021

Capítulo 1

Saque el máximo partido a la plataforma Linux



Razones para elegir Linux

Las empresas de TI se enfrentan a la enorme presión de implementar y gestionar los servicios y las soluciones a un ritmo vertiginoso y, por lo general, con escasos recursos y habilidades. Para realizar esta tarea con éxito, las cargas de trabajo de TI deben contar con una confiabilidad y disponibilidad uniformes, así como con funciones centradas en la seguridad. En este contexto es donde interviene Linux.

Se convirtió en la plataforma estándar para desarrollar y ejecutar las cargas de trabajo más importantes en el centro de datos, en un entorno de nube o en el extremo de la red. Las empresas de diversos sectores e industrias utilizan estas soluciones para poner sus entornos de TI al servicio de la innovación.

Importancia de la distribución de Linux

Para garantizar el éxito de su entorno de TI es de vital importancia determinar la distribución de Linux que utilizará su empresa y elegir el sistema operativo general, ya que una decisión acertada puede influir notablemente en la eficacia, el rendimiento, la seguridad y los costes operativos de su entorno.

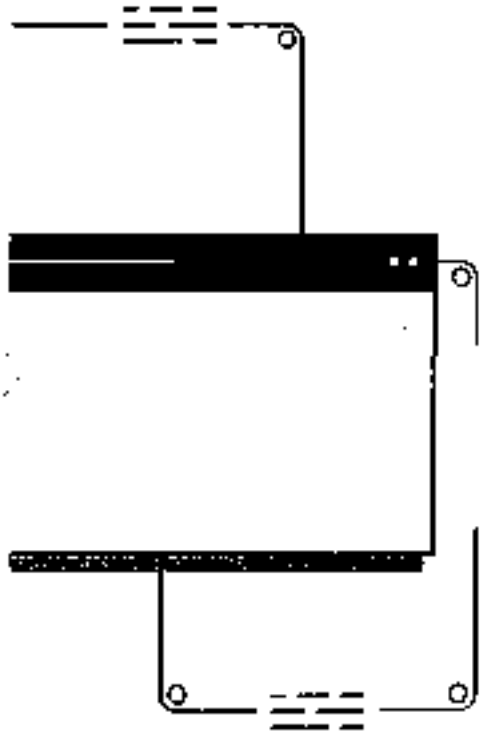
El uso de una plataforma open source adecuada puede favorecer el crecimiento a largo plazo. Si su equipo tiene la capacidad de aplicar las habilidades que ya posee en distintos entornos, la empresa podrá hacer frente a las demandas cambiantes y admitir cargas de trabajo nuevas con mayor facilidad. De ese modo, se mejorará la experiencia de los empleados y los clientes y, al mismo tiempo, se dará soporte a una gran variedad de casos prácticos, sistemas de destino y dispositivos.

Cada distribución presenta una serie de ventajas y desventajas. Por ello, debe sopesar sus opciones en función de la adecuación de las funciones, las integraciones, las asociaciones y la experiencia del servicio de soporte a las necesidades de su empresa.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

Consejos para elegir la plataforma Linux adecuada

Para crear una infraestructura de TI moderna que respalde la innovación y los objetivos a largo plazo, hay cuatro áreas importantes que debe tener en cuenta al seleccionar su plataforma Linux. En tal caso, se recomienda una plataforma con las siguientes características



Operaciones optimizadas: si cuenta con la plataforma Linux adecuada, podrá agilizar las operaciones para que sus equipos no tengan que dedicar tanto tiempo al mantenimiento y puedan centrarse más en generar innovaciones y aportar valor. Busque una plataforma que se haya diseñado para el entorno de nube híbrida y que permita a los equipos desarrollar, implementar y adaptar los sistemas sin necesidad de realizar cursos de capacitación adicionales. Además, debe disponer de herramientas de gestión para las tecnologías nuevas y las que ya tiene, así como de funciones de automatización integradas que simplifiquen la implementación, la ampliación y la gestión de las aplicaciones cuando estén en producción.

Reducción de los riesgos: opte por una distribución con funciones que reduzcan los riesgos de seguridad y cumplimiento y faciliten la resolución de los problemas que pudieran derivarse de ellos. Además, utilice una plataforma que cumpla los estándares gubernamentales y del sector en materia de validaciones y certificaciones, y que aplique las prácticas recomendadas de desarrollo para reducir las fallas de seguridad en su código antes de distribuirlo. Elija una solución que le ayude a reducir las amenazas nuevas al simplificar los procesos de detección y gestión.

Simplificación de la infraestructura: es recomendable que elija una solución Linux que aumente la eficacia operativa, ya que la complejidad de la infraestructura reduce la eficiencia de la TI e incrementa los costos de gestión, lo cual limita la innovación a largo plazo. Si cuenta con una plataforma compatible con un amplio catálogo de hardware, software y asociaciones en la nube, podrá acelerar las innovaciones e impulsar la agilidad. Descubra el modo de utilizar el análisis predictivo para reducir el tiempo dedicado a las tareas operativas complejas, que permite detectar problemas de manera anticipada, analizar las configuraciones y determinar las soluciones adecuadas.

Estrategia para el futuro: aspire a lograr el éxito a largo plazo con una solución Linux que ofrezca la estabilidad y la durabilidad que necesita para gestionar las aplicaciones más importantes durante al menos 10 años. Opte por una plataforma con ciclos de lanzamiento predecibles, fechas de finalización del mantenimiento, opciones de actualización y compatibilidad para poder replicar pasos con antelación. La plataforma también debe disponer de herramientas de migración y automatización que simplifiquen el proceso para trasladarse a la versión más reciente o desde otras distribuciones. Por último, tenga en cuenta la importancia del servicio de asistencia y las interacciones y elija una solución que ofrezca soporte técnico permanente y un amplio ecosistema de partners de software y hardware.

Más información sobre los aspectos más importantes de la plataforma Linux

Obra protegida por derechos de autor
EMDOC CONSULTORES
Santo Domingo, R.D.

Aumento de la agilidad con un enfoque de nube híbrida y el uso de contenedores

Aunque la competencia incesante y los estándares de cumplimiento en constante cambio obligan a las empresas a evolucionar, las infraestructuras tradicionales y poco flexibles añaden una complejidad que, a menudo, ralentiza todo intento de avance.

En este contexto, los equipos de TI son los encargados de facilitar a los desarrolladores los recursos que necesitan para transformar rápidamente una simple idea en una iniciativa que aporte valor a la empresa; sin embargo, esta tarea ingente puede plantear numerosos desafíos. Además, se espera que los equipos mantengan el control, la seguridad y la confiabilidad de la infraestructura sin provocar obstáculos en el ciclo de vida del desarrollo.

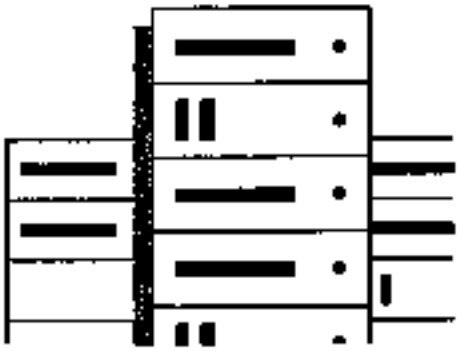
La combinación de los entornos de nube híbrida y las tecnologías desarrolladas en la nube (por ejemplo, los microservicios Kubernetes y los contenedores de Linux) ofrece a los equipos de TI la agilidad y portabilidad que necesitan para prestar servicios a los desarrolladores y a las líneas de negocio.

En su afán por modernizar las TI, la seguridad y la gestión ocupan un lugar primordial en las agendas de las empresas actuales. En efecto, la seguridad de la TI es una de las principales prioridades en materia de financiación para prácticamente la mitad de las empresas (46 %), a la que siguen la gestión de la nube y la TI (38 %), la infraestructura de nube (35 %) y la automatización de las operaciones de TI (29 %)[1].



Con Red Hat® Enterprise Linux®, podrá disfrutar de las funciones de seguridad y los controles de gestión avanzados que requieren las implementaciones de la nube híbrida y, al mismo tiempo, obtener una mayor estabilidad, confiabilidad y rendimiento. Por su parte, Red Hat OpenShift® es una plataforma Kubernetes empresarial líder en el sector que simplifica la organización en contenedores para las aplicaciones en la nube y brinda a los desarrolladores las herramientas adecuadas para mejorar su productividad y su capacidad de innovación.

Consulte Potencie la agilidad con los contenedores y la nube híbrida para obtener más información sobre las soluciones de nube híbrida de Red Hat: RedHat Enterprise Linux, Red Hat OpenShift y Red Hat Enterprise Linux CoreOS. Estas soluciones open source ofrecen a las compañías una infraestructura eficiente, ininterrumpida, adaptable y dinámica sin comprometer los requisitos normativos y financieros.



Para finales de año, el 70 % de todas las cargas de trabajo empresariales se implementarán en los servicios de infraestructura y plataformas en la nube, mientras que en 2020 esta cifra era del 50 %.

[1] Red Hat. "2022 Global Tech Outlook: un informe de Red Hat". Noviembre de 2021.
[2] Gartner. "Hype Cycle" for Cloud Security, 2021". 27 de julio de 2021.

CONSORCIO EMDOC
EMDOC
CONSORCIO
7
Santo Domingo, R.D.

Capítulo 2

Ventajas de Linux

Para alcanzar los objetivos de su empresa, es esencial contar con un sistema operativo confiable que sea compatible con todas las aplicaciones de su infraestructura y que pueda configurarse e implementarse según sea necesario y, al mismo tiempo, garantice el ciclo de vida y la seguridad.

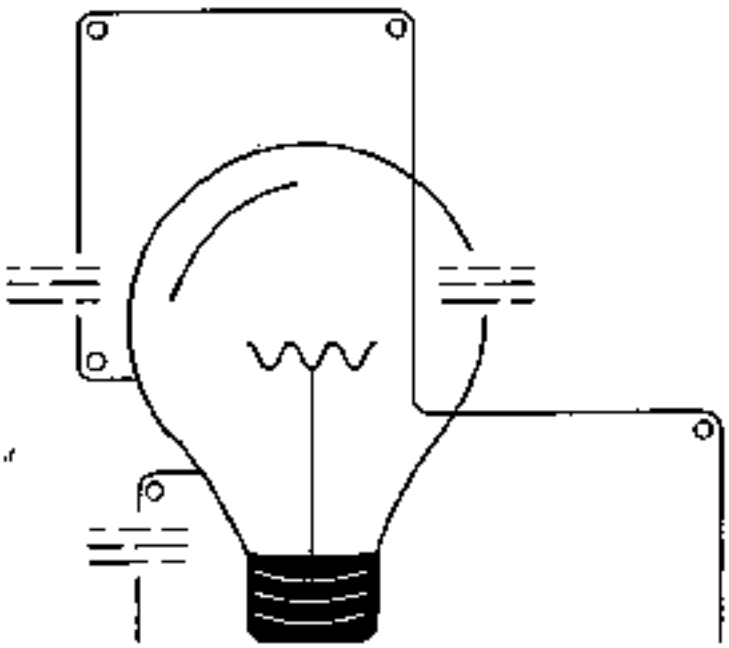
Con Red Hat Enterprise Linux, su empresa puede obtener mayor flexibilidad, funciones de seguridad y uniformidad en los entornos de nube híbrida, lo cual fomentará la innovación y la eficiencia.

Ayuda para la estandarización en todos sus entornos

Red Hat Enterprise Linux ofrece a las empresas la posibilidad de estandarizar los entornos de nube híbrida, ya sean virtualizados, en las instalaciones, en la nube pública o en el extremo de la red. Frente a las presiones normativas y de la competencia actuales, las empresas deben contar con una plataforma que brinde una experiencia de gestión y desarrollo optimizada, así como herramientas que les permitan diseñar, gestionar y ajustar sus entornos de manera uniforme y en todas partes.

Aceleración de la innovación dondequiera que se produzca

Con Red Hat Enterprise Linux como base, el departamento de TI puede dedicar menos tiempo a mantenimiento de los entornos de nube híbrida y centrarse más en las cargas de trabajo y las aplicaciones que aportan valor a la empresa, condequiera que se implementen. La automatización integrada para gestionar las tareas repetitivas y redundantes reduce el tiempo que se dedica a implementar, ajustar y gestionar las aplicaciones en la fase de producción. Asimismo, los procesos manuales automatizados en torno a actividades como la implementación de funciones de seguridad, las actualizaciones, la aplicación de parches y los cambios de configuración pueden reducir los puntos vulnerables que suelen producirse por los errores humanos.



CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD



Una base estable y centrada en la seguridad

Red Hat Enterprise Linux ofrece la estabilidad, la uniformidad y la confianza necesarias para crear una base sólida que se centre en la seguridad. Se pueden ampliar las aplicaciones nuevas y adoptar las tecnologías incipientes con la seguridad de que la empresa cumple los requisitos normativos y del sector. Asimismo, los controles integrados y automatizados supervisan la infraestructura de TI, de modo que las nuevas amenazas se detectan y resuelven con mayor facilidad y, al mismo tiempo, se gestionan el cumplimiento de normativas, el rendimiento, la disponibilidad y la estabilidad.

Operaciones seguras

La combinación de un amplio ecosistema de software, hardware y entornos de nube, las opciones de soporte integral durante un ciclo de vida prolongado y las herramientas integradas de desarrollo, gestión y seguridad sitúan a Red Hat Enterprise Linux entre las plataformas más confiables para impulsar la innovación y el rendimiento en entornos de nube híbrida.

CONSORCIO EMDOC
EMDOC
Santo Domingo, R.D.

Capítulo 3

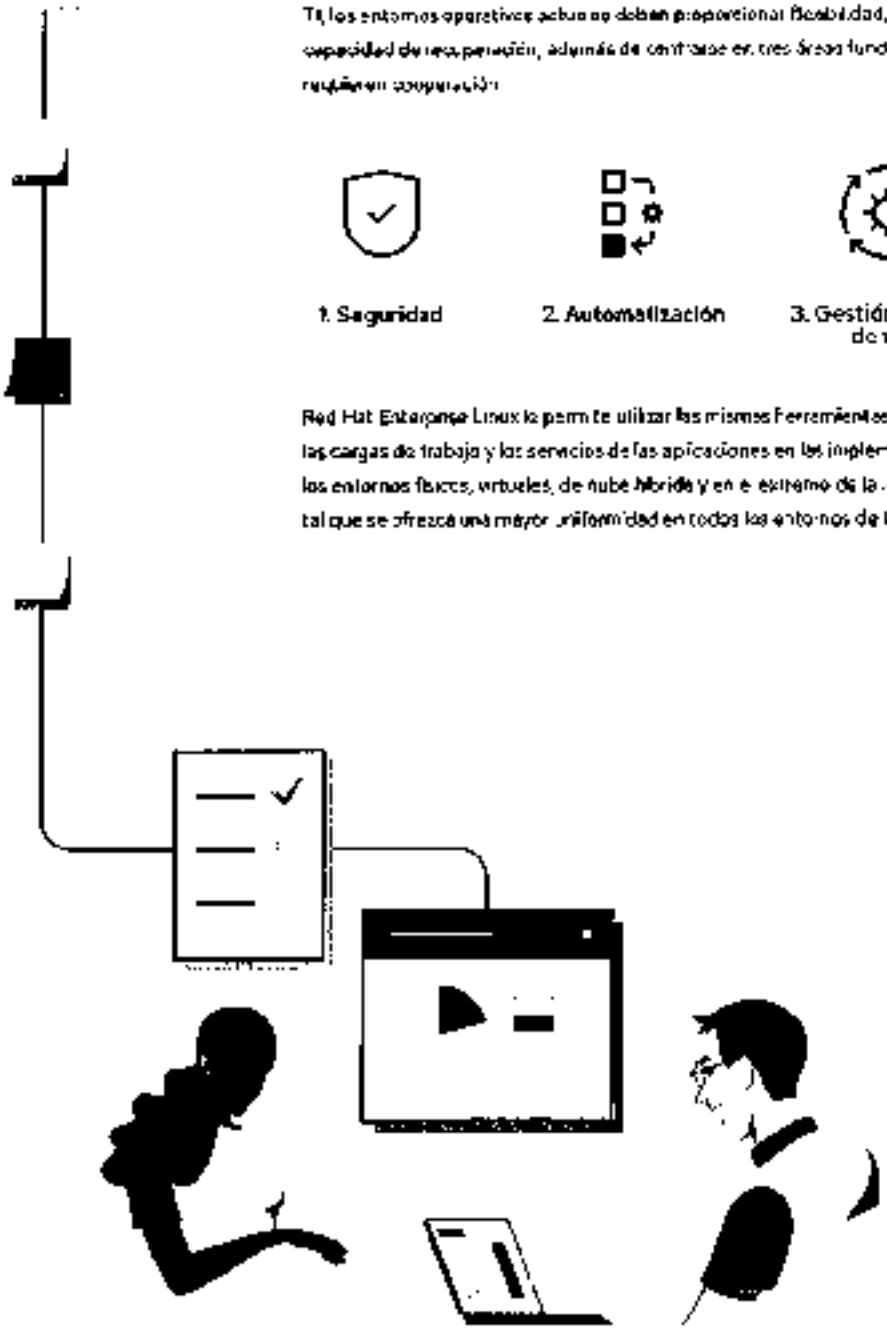
El enfoque de Red Hat

Diseñe y gestione su entorno de nube híbrida con soluciones centradas en la seguridad y la obtención rápida de resultados

Red Hat Enterprise Linux crea una base valiosa para la infraestructura de TI moderna. Para satisfacer las necesidades empresariales a las que se enfrentan los equipos de TI, los entornos operativos actuales deben proporcionar flexibilidad, uniformidad y capacidad de recuperación, además de centrarse en tres áreas fundamentales y que requieren cooperación:

1. Seguridad
2. Automatización
3. Gestión del ciclo de vida

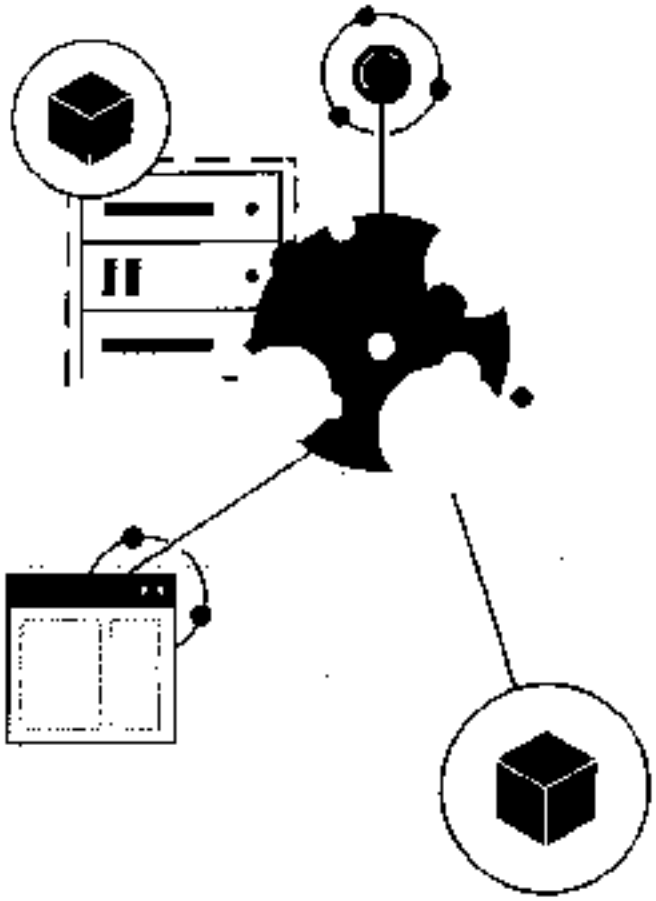
Red Hat Enterprise Linux le permite utilizar las mismas herramientas para gestionar las cargas de trabajo y los servicios de las aplicaciones en las implementaciones de los entornos físicos, virtuales, de nube híbrida y en el extremo de la red de manera tal que se ofrezca una mayor uniformidad en todos los entornos de la empresa.



CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

Más que un sistema operativo: una base de desarrollo

Con Red Hat, las empresas pueden implementar una stack completa de tecnologías open source de alto rendimiento y, al mismo tiempo, reducir las dificultades y los costos de implementación y agilizar la obtención de resultados. Cuando se utiliza como base para productos como Red Hat Ansible® Automation Platform, Red Hat OpenShift y otras soluciones y servicios de la marca, Red Hat Enterprise Linux ofrece funciones de seguridad, rendimiento, interoperabilidad y ventajas de innovación que se extienden a toda la infraestructura

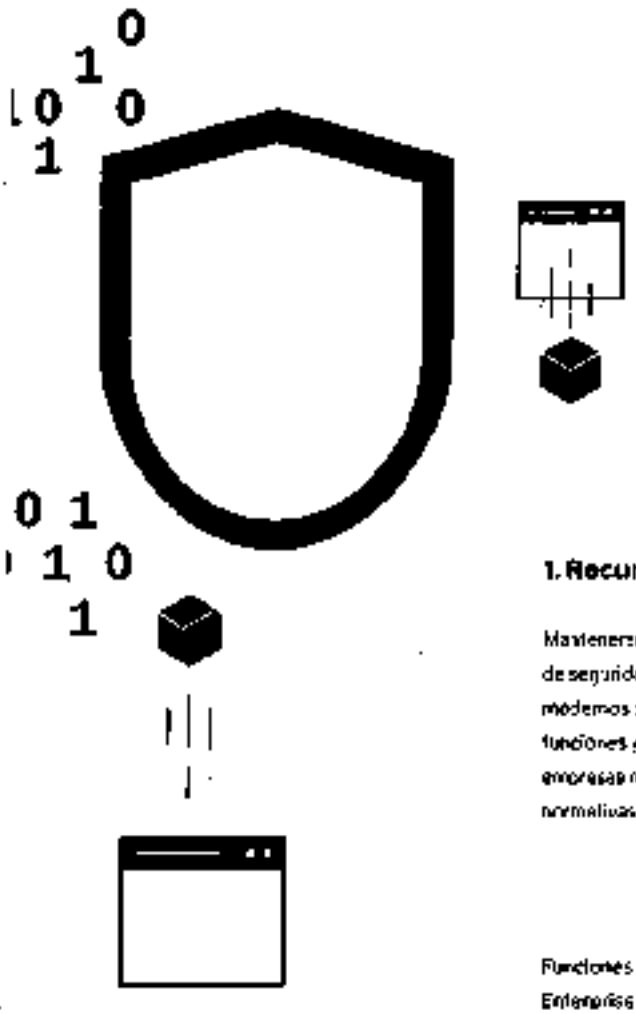


Seis ventajas de utilizar Red Hat Enterprise Linux

La plataforma aporta ventajas en seis áreas fundamentales:

- Recursos y herramientas de seguridad
- Diseño sencillo para los desarrolladores
- Análisis y resolución integrada de problemas
- Gestión y automatización optimizadas
- Flexibilidad y soporte a largo plazo para el ciclo de vida
- Asociaciones y certificaciones

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.



1. Recursos y herramientas de seguridad integrados

Mantenerse al día con las últimas tendencias y las prácticas recomendadas en materia de seguridad no es una tarea sencilla y, a menudo, la adopción de enfoques DevSecOps modernos puede agravar estos desafíos. Sin embargo, Red Hat Enterprise Linux ofrece funciones y certificaciones de seguridad integradas que simplifican el modo en que las empresas reducen los puntos vulnerables mientras garantizan el cumplimiento de las normativas y la seguridad según sea necesario.

Funciones de seguridad de Red Hat Enterprise Linux:

- Equipo de seguridad exclusivo, un sistema de software para el análisis y la resolución de problemas, y el acceso continuo a recursos nuevos para que pueda garantizar el cumplimiento de las normativas.
- Herramientas de seguridad automatizadas, calificaciones de seguridad periódicas y ejecución activa de parches, y el acceso a especialistas que le ayudarán a mantener su entorno de TI actualizado y centrado en la seguridad.
- Certificación que cumple los estándares estrictos de seguridad, como los Estándares Federales de Procesamiento de la Información (FIPS) publicación 140-2; Common Criteria (CC); y las Guías de Implementación Técnica de Seguridad (STIG), y una cadena de suministro de software confiable que brinden la seguridad y la tranquilidad necesarias en todos los sectores y casos prácticos.
- Acceso a la ejecución activa de los parches en el kernel para los puntos vulnerables y las exposiciones comunes (CVE) graves sin costo adicional, lo cual permite reducir el tiempo de inactividad sin comprometer la seguridad.
- Una suscripción a Red Hat Insights que permite a las empresas crear políticas para el Protocolo de Automatización del Contenido de Seguridad (SCAP) y realizar un rápido análisis del sistema para garantizar el cumplimiento normativo.

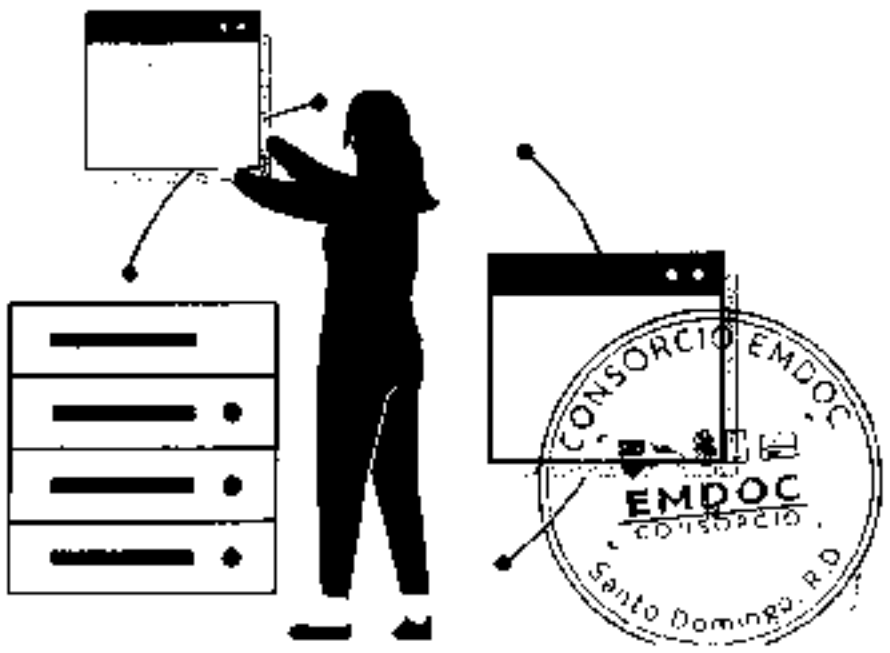
CONSORCIO EMDOC
EMDOC
Santo Domingo, R.D.

2. Los flujos de aplicaciones ofrecen un entorno sencillo para los desarrolladores

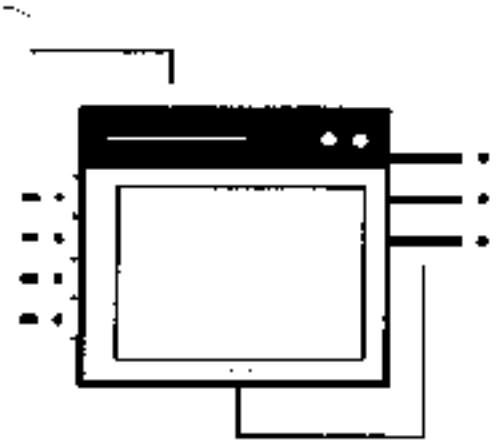
Red Hat Enterprise Linux impulsa la agilidad de los desarrolladores y proporciona un entorno de producción estable. Además, incluye funciones y herramientas que aceleran los procesos de desarrollo de las aplicaciones, como la selección de herramientas, la codificación, la instalación y la configuración.

Funciones de desarrollo de Red Hat Enterprise Linux:

- Una amplia selección de lenguajes de programación y tiempos de ejecución, compiladores, bases de datos open source, servidores web y de caché, y herramientas de desarrollo nuevos disponibles a través de los flujos de aplicaciones (AppStreams) para facilitar su desarrollo e implementación.
- AppStreams distribuidos y actualizados con frecuencia que ofrecen las versiones estables más recientes de los lenguajes, las herramientas y las bases de datos que necesitan los desarrolladores cuando con soporte a los equipos que utilizan una versión anterior.
- Acceso a diversas herramientas para el desarrollo en contenedores, como Buildah para crear contenedores, Podman para ejecutarlos y Skopeo para compartirlos.



CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.



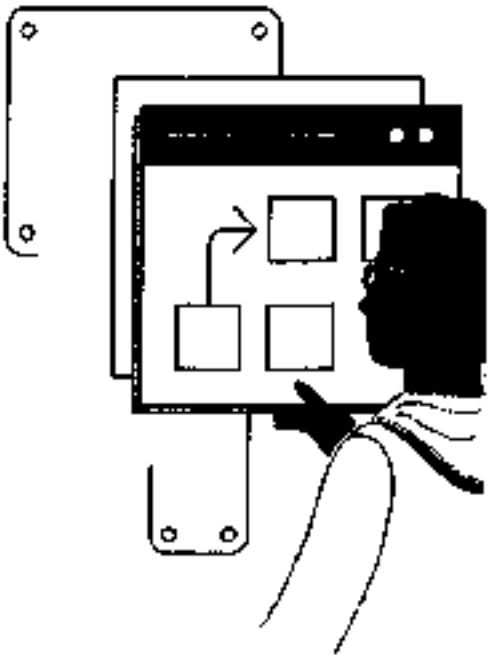
3. Red Hat Insights para el análisis y la resolución de problemas

Todas las suscripciones a Red Hat Enterprise Linux incluyen Red Hat Insights, la oferta de software como servicio (SaaS) que permite identificar y corregir los problemas de cada entorno con antelación. Recopila el análisis de los datos de toda la empresa y proporciona información práctica para mejorar la eficiencia y la confiabilidad.

Además, pone a las funciones de seguridad al ofrecer alertas sobre los puntos vulnerables de manera permanente y orientación específica para que pueda optimizar el tiempo de actividad y evitar problemas relacionados con la protección de los datos, la falta de cumplimiento de las configuraciones, los sistemas sin parches y el impacto de los desajustes de la configuración en DevOps, los interesados de la seguridad de la nube.

4. Automatización para agilizar la gestión

Red Hat Enterprise Linux agiliza la gestión del sistema operativo y simplifica las tareas diarias de administración, lo cual brinda una experiencia uniforme y constante gracias a la estandarización y automatización de los flujos de trabajo repetibles. Se integra con Red Hat Ansible Automation Platform y Red Hat Smart Management para proporcionar funciones flexibles y eficaces de automatización y gestión de infraestructuras.



Red Hat Enterprise Linux incluye:

- Herramientas integradas de automatización del flujo de trabajo compatibles con las herramientas avanzadas de gestión y automatización de Red Hat para facilitar la administración de su entorno híbrido.
- Funciones del sistema: un conjunto de flujos de trabajo que los suscriptores pueden utilizar para configurar las interfaces y ejecutar las tareas de manera rápida y uniforme en diferentes versiones de Red Hat Enterprise Linux y con el mismo playbook de automatización.
- Acceso a Red Hat Smart Management y Red Hat Ansible Automation Platform para preparar los sistemas, aplicarles parches, configurarlos y supervisarlos de manera más eficaz, así como probarlos y producirlos según sea necesario.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.



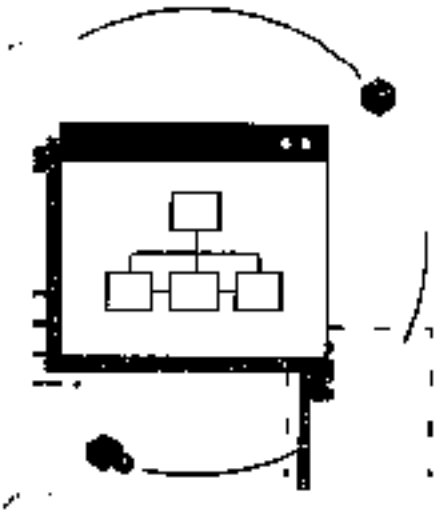
5. Flexibilidad y soporte para el ciclo de vida

Red Hat Enterprise Linux cuenta con varias versiones compatibles y ofrece la plataforma sostenible, flexible, estable y centrada en la seguridad adecuada para satisfacer las necesidades de su empresa. Además, le permite actualizar y adoptar nuevas funciones en el momento oportuno y cuando así se requiera. Red Hat le permite simplificar la planificación de la TI al difundir los ciclos de lanzamiento a largo plazo y las opciones del ciclo de vida.



Funciones de soporte de Red Hat Enterprise Linux:

- Una frecuencia de lanzamientos predecible y pública que ofrece hasta diez años de actualizaciones y soporte para las versiones principales y dos años para las versiones secundarias.
- Una versión uniforme del kernel para cada versión principal y las versiones secundarias asociadas, lo cual garantiza la estabilidad de la aplicación y el hardware durante todo su ciclo de vida.
- Herramientas integradas de actualización para que pueda migrar a las versiones más recientes de Red Hat Enterprise Linux de forma más eficaz cuando desee hacerlo.

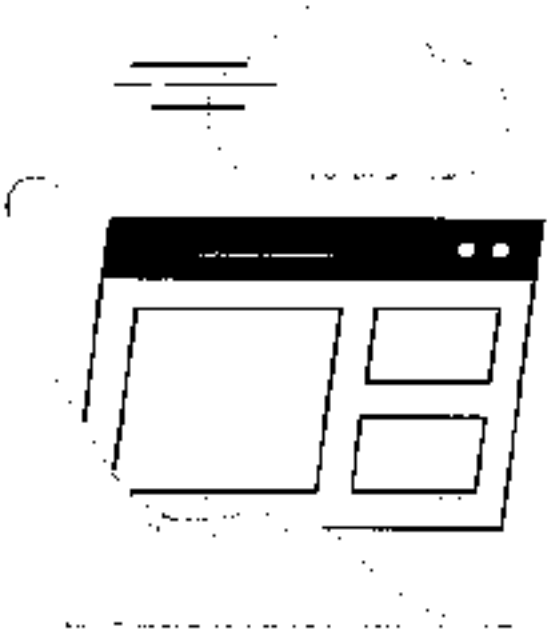


6. Un ecosistema de asociaciones y certificaciones

Red Hat se asocia con los líderes del sector en hardware y software, y cuenta con la certificación correspondiente para que se pueda utilizar con los principales proveedores de nubes, de modo que usted obtenga mayor flexibilidad, más estabilidad y una capacidad de innovación sin precedentes. Por ello, el equipo de Red Hat cree un amplio ecosistema de partners certificados para que las empresas puedan elegir las tecnologías, los productos y las plataformas que les resulten más eficaces para alcanzar sus objetivos, con la seguridad de que funcionarán con Red Hat Enterprise Linux sin ningún tipo de inconveniente.

Entre sus principales partners se encuentran SAP, Microsoft, Intel, Dell Technologies, Google y AWS.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD



Conozca las ventajas que ofrece Red Hat Enterprise Linux

Acceda a una suscripción gratuita de 60 días a Red Hat Enterprise Linux Server y aproveche todo el potencial de su infraestructura de TI. Obtendrá acceso a Red Hat Smart Management y Red Hat Insights, así como al Portal de clientes galardonado de Red Hat, en el cual encontrará documentación, foros de debate, videos útiles para dar los primeros pasos y mucho más.

Comience a probar hoy mismo



Acerca de Red Hat

Red Hat® es el proveedor líder mundial de soluciones de software open source para empresas, que ha adoptado un enfoque impulsado por la comunidad para ofrecer tecnologías confiables y de alto rendimiento de Linux, nube híbrida, contenedores y Kubernetes. Red Hat ayuda a los clientes a integrar las aplicaciones de TI nuevas y actuales, desarrollar aplicaciones nativas de la nube, estandarizar nuestro sistema operativo líder del sector, y automatizar, proteger y gestionar entornos complejos. Sus servicios galardonados de consultoría, capacitación y compatibilidad convierten a Red Hat en asesor de confianza para las empresas de la lista Fortune 500. Como partner estratégico de proveedores de nube, integradores de sistemas, proveedores de aplicaciones, clientes y comunidades open source, Red Hat ayuda a las empresas a prepararse para el futuro del mundo digital.



facebook.com/redhatinc
@RedHatLatam
@RedHatIberia
linkedin.com/company/red-hat

ARGENTINA
-5411 4329 7300

CHILE
+562 2597 7000

COLOMBIA
+571 508 8631
+52 55 8851 6400

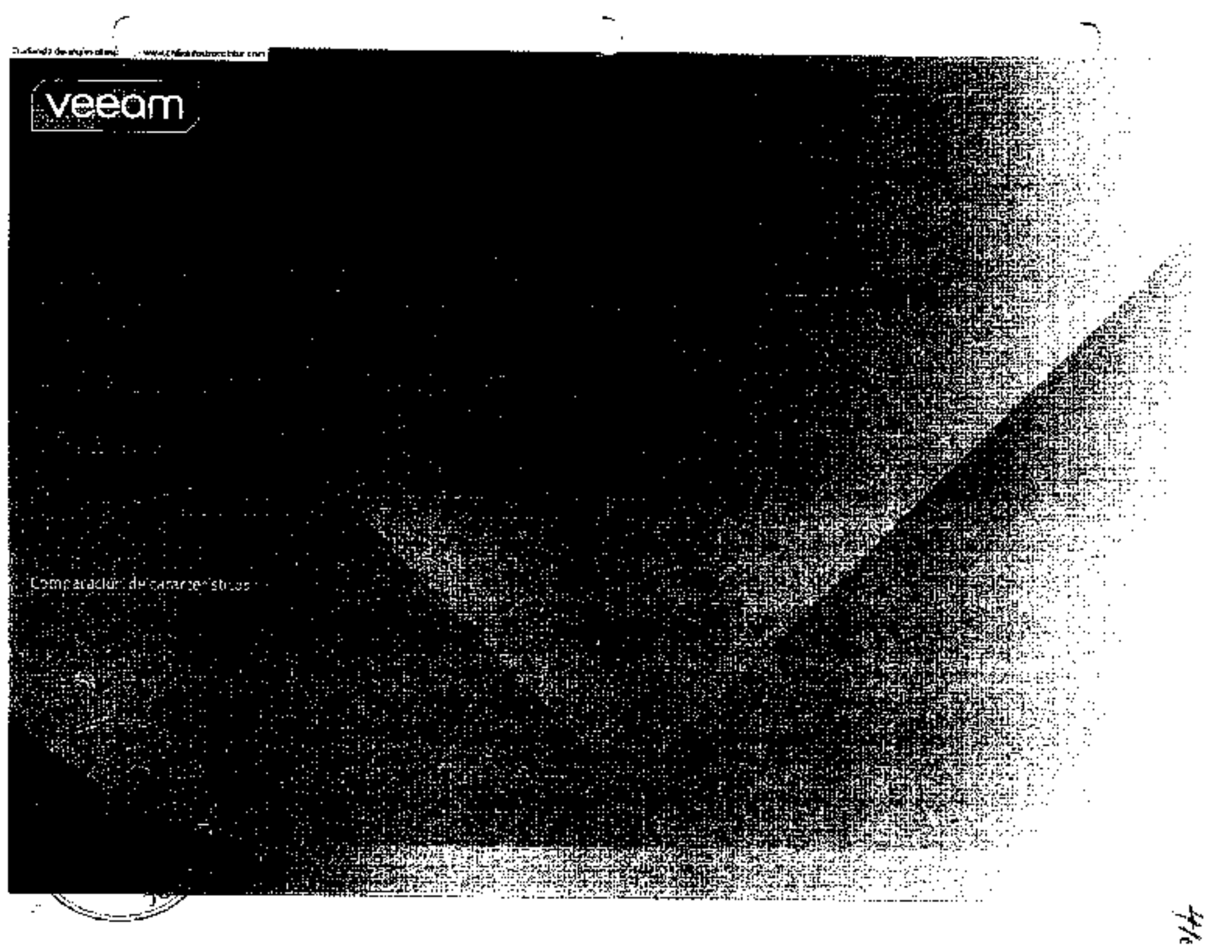
MÉXICO
+52 55 8851 6400

ESPAÑA
+34 914 148 300

es.redhat.com
#P3HP05_0722

Copyright © 2022 Red Hat, Inc. Red Hat, el logotipo de Red Hat, Ansible y OpenShift son marcas comerciales o registradas de Red Hat, Inc. o sus subsidiarias en Estados Unidos y en otros países. Linux® es la marca comercial registrada de Linus Torvalds en Estados Unidos y en otros países. Gartner y Magic Quadrant son marcas comerciales y marcas de servicio registradas de Gartner, Inc. o de sus filiales en Estados Unidos y en todo el mundo y que utilizamos en el presente con el debido consentimiento. Todos los derechos reservados.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.


veeam
Comparaclon de caracteristicas

Contenido

Detalles de la licencia 3

Licencias para proveedores de servicios gestionados y en la nube de Veeam (VCSP) 3

Copia de seguridad y recuperación
Desarrollado por Veeam Backup & Replication™ 5

Seguridad 5

Respaldo 7

Copia de seguridad para workloads en la nube 9

Compatibilidad con copia de seguridad de SAN/Direct NFS 10

Almacenamiento de copias de seguridad 10

Replicación 13

Restaurar 14

Recuperación empresarial 14

Recuperación a nivel de archivos y elementos 14

Herramientas de suite 16

Autoservicio 17

Gestión 18

Monitoreo y análisis
Desarrollado por Veeam ONE™ 19

Seguimiento y presentación de informes 19

Monitoreo y alertas para la nube híbrida 20

Monitoreo y alertas para infraestructura virtual 20

Personalización y automatización de informes y alarmas 21

Gobernanza y cumplimiento 22

Automatización inteligente 22

Panel de control 22

Planificación de capacidad 22

Contracargo y facturación 23

Orquestación de recuperación
Desarrollado por Veeam Recovery Orchestrator 24

Documentación y automatización de la recuperación 24

Pruebas de carga y generación de informes 25

CONSORCIO EMDOC

© 2024 Veeam Software. Todos los derechos reservados. Todas las demás marcas comerciales son propiedad de sus respectivos dueños.

Plataforma de datos de Veeam Veeam ofrece varias opciones empaquetadas para brindar seguridad incansable, recuperación rápida y confiable y total libertad de datos. Ya sea que recién esté comenzando o esté administrando una gran operación empresarial, Veeam tiene una opción flexible para usted. La licencia universal de Veeam (VUL) es una licencia portátil innovadora que le permite la flexibilidad de proteger cargas de trabajo físicas, virtuales y en la nube de manera intercambiable sin importar en qué parte de su transición híbrida se encuentre.
Las funciones de backup, monitoreo y recuperación extremadamente capaces de Veeam Data Platform están listas para mantener su negocio en funcionamiento.

Detalles de la licencia

La licencia universal de Veeam (VUL) portátil y con todas las funciones es la forma en que se licencia Veeam Data Platform, lo que permite el soporte en cualquier entorno, ya sea local o en implementaciones híbridas o multinube, incluida la capacidad de funciones completas para todos los tipos de cargas de trabajo, incluidos VMware, Hyper-V, AWS, Azure, Google Cloud, Windows, Linux, macOS, Nutanix, Oracle Linux Virtualization Manager, Red Hat Virtualization, Proxmox VE y mucho más. Este documento describe las funciones que están disponibles en la edición adecuada de Veeam Data Platform.

Si necesita detalles para hacer referencias cruzadas de licencias heredadas basadas en sockets que dejaron de venderse en 2023, consulte este artículo.

Cargas de trabajo	Licencia universal de Veeam
Entornos	Implementaciones en la nube y híbridas
Máquinas virtuales: VMware vSphere, Microsoft Hyper-V, Nutanix AHV, Oracle Linux Virtualization Manager, Red Hat Virtualization y Proxmox VE	Sí
Mejorado Servidores físicos, estaciones de trabajo y puntos finales: Windows, Linux, macOS, Oracle Solaris e IBM AIX	Sí
Mejorado Aplicaciones empresariales para Microsoft, Oracle, SAP HANA, MongoDB y más	Sí
Mejorado Copias de seguridad y recuperación nativas de la nube para AWS, Microsoft Azure y Google Cloud	Sí
Mejorado Copias de seguridad de contenedores de Kubernetes y aplicaciones de Kubernetes	Sí
¡Habrá más!	

Licencias para proveedores de servicios gestionados y en la nube de Veeam (VCSP)

Las licencias de alquiler de VCSP funcionan de manera similar a las licencias de suscripción, pero utilizan un sistema basado en puntos cuyo consumo depende de los niveles de capacidad. Para obtener más información, consulte su Documentación de licencias de VCSP o hable con su proveedor de servicios. Los proveedores de servicios pueden acceder a la Comparación de funciones de VCSP y guía sobre ProPortal de socios.

Copyright © 2024 Veeam Software. Todos los derechos reservados. Todas las demás marcas comerciales son propiedad de sus respectivos dueños.

COMERCIO EXTERIOR MADOC

Veeam Data Platform

	Zero Trust DataResilience		Generative AI	Detect + Identify Threats		Security and Observability				Recovery Orchestration and Compliance		
	Data Protection & Verified Recovery		AI Assistant	AI-powered Malware Detection	Proactive Threat Hunting	Security Integrations	Analytics, Discovery & Reporting	Intelligent Diagnostics & Remediation	Threat Health Center	Orchestrated Recovery & Validation	GRC Audit Documentation	Forensic Triage
Foundation	✓		✓	✓	—	—	—	—	—	—	—	—
Advanced	✓		✓	✓	✓	✓	✓	✓	✓	—	—	—
Premium	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

+ veeam

- Coveware Incident Response Subscription
- Up to $5M Ransomware Warranty
- 24/7/365 SWAT Team with 30min SLA to help
- Onboarding, Implementation, Quarterly Health Assessments for Security Best Practices

CONSORCIO EMDOC

[redacted]

Comparación de funciones de Veeam Data Platform

✔ Disponible en esta edición ✔ Funcionalidad ampliada

Copia de seguridad y recuperación *Desarrollado por Veeam* *Copia de seguridad y replicación*	Comunidad	Plataforma de datos de Veeam Licencia universal de Veeam (VUL) Básica	Avanzada	Premium	Descripción
Seguridad					
NuevaDetección de malware		✔	✔	✔	Escanee y analice todos los datos de copia de seguridad en busca de malware durante el proceso de copia de seguridad. Utilice el motor de detección de malware de Veeam para buscar indicadores de malware conocidos y comparar los datos nuevos con los patrones de ransomware detectados anteriormente, lo que le ayuda a garantizar que sus copias de seguridad siguen siendo recuperables y limpias. (*YARA Scan requiere la edición Avanzada o Premium*)
NuevoEscaneo YARA			✔	✔	La nueva opción Content Scan disponible en SureBackup, Secure Restore y Scan Backup Function proporciona un nivel adicional de seguridad al escanear copias de seguridad completas con el motor YARA en función de las reglas de detección elegidas. Se puede utilizar Malwarebytes para identificar rápidamente la amenaza conocida o para realizar una búsqueda basada en patrones. (*YARA Scan requiere Advanced Edition o Premium Edition*)
NuevaAplicación Veeam para Splunk			✔	✔	Aproveche las capacidades de reenvío de eventos de Veeam. La aplicación Veeam para Splunk incluye paneles de control / seguridad, alertas de seguridad e informes. La aplicación se integra perfectamente con los roles de usuarios y la gestión de ubicaciones de Splunk.
NuevaAplicación Veeam para Palo Alto Networks XSIAM			✔	✔	Aproveche las capacidades de reenvío de eventos de Veeam tanto de Veeam Backup & Replication como de Veeam ONE. La aplicación Veeam para Palo Alto XSIAM incluye paneles de control y reportes de seguridad y monitoreo. También se integra con la gestión de usuarios y el reconocimiento de ubicación de Palo Alto. (PRÓXIMAMENTE)
NuevaAplicación Veeam para Palo Alto Networks XSOAR			✔	✔	Ofrece una integración bidireccional a nivel de API con Veeam Backup & Replication y Veeam ONE para equipos de automatización y SOC. Proporciona creación automática de incidentes, un panel de seguridad basado en indicadores de seguridad de Veeam y permite la resolución de incidentes directamente desde la interfaz de usuario de XSOAR. (PRÓXIMAMENTE)
NuevoReenvío de eventos de Syslog		✔	✔	✔	Los eventos de Veeam se pueden transferir a servidores syslog externos, incluidas herramientas SIEM de terceros compatibles con syslog que monitorizan eventos corporativos y entienden el soporte de sus equipos de seguridad.
Mejoras en la interfaz de Veeam		✔	✔	✔	Experimente una experiencia de usuario mejorada con una interfaz de usuario actualizada de Veeam Backup & Replication para una navegación más fluida y una experiencia de usuario mejorada en general.
[illegible]		✔	✔	✔	La autorización de Four Eyes requiere que un segundo usuario autorice ciertas operaciones confidenciales relacionadas con la eliminación de copias de seguridad o la eliminación de repositorios en Veeam Backup & Replication. Se incorporación de nuevos administradores, la modificación de usuarios autorizados o los cambios en roles.

[illegible] Todos los derechos reservados. Todas las marcas comerciales son propiedad de sus respectivos dueños.

Comparación de funciones de Veeam Data Platform

✔ Incluido en la edición ✔ No incluido en la edición

Capas de seguridad y recuperación Desarrollado por Veeam Capas de seguridad y recuperación	Comunidad	Plataforma de datos de Veeam Licencia universal de Veeam (VUL) Base	Avanzado	Premium	Descripción
Mejora de la integración del sistema de gestión de claves (KMS)			✔	✔	Administre de forma centralizada las claves criptográficas, eliminando la complejidad de una administración de claves específica de la aplicación. (Requiere el plan de Advanced o Premium para esta funcionalidad)
Restauración segura		✔	✔	✔	Aumente la seguridad y reduzca las interrupciones causadas por malware y recupere un punto de restauración seguro y sin violaciones mediante un análisis YARA opcional integrado directamente en los archivos de respaldo antes de la recuperación. (*YARA Scan requiere Advanced o Premium Edition).
SureBackup: recuperación segura		✔	✔	✔	Obtenga funciones automatizadas, prueba y verifique la usabilidad de cada copia de seguridad y réplica de la máquina virtual exactamente antes de un evento de caída de seguridad en una sandbox aislada de su entorno de producción, incluida la compatibilidad con scripts de prueba de aplicaciones personalizados. Realice análisis de malware opcionales y activos* para copias de seguridad sospechosas o cargas de trabajo. (*YARA Scan requiere Advanced o Premium Edition).
NureAshrena potenciado por IA de Veeam		✔	✔	✔	Aclaraciones inmediata en el producto mediante la generativa impulsada por grandes modelos de lenguaje, capacitada en la documentación del producto con acceso en tiempo real a la base de conocimiento de Veeam.
Inmutabilidad	✔	✔	✔	✔	La inmutabilidad la proporcionan el repositorio reforzado para todas las ediciones.
Autenticación multifactor (MFA)		✔	✔	✔	Mejore el control de acceso de Veeam Backup & Replication, habilitando la autenticación multifactor para los usuarios en la consola de respaldo.
Implementación en sistemas que solo utilizan kernel	✔	✔	✔	✔	Lleve la seguridad a un nuevo nivel con la posibilidad de ejecutar todos los componentes de Veeam en entornos solo kernel.
Seguridad de Veeam y Asesor de cumplimiento	✔	✔	✔	✔	Realice una verificación automatizada de la configuración del servidor de respaldo de Veeam para obtener pautas de mejores prácticas para comprender cómo se puede mejorar la endurecimiento de respaldo para abordar posibles problemas de seguridad.
Despliegue en entornos IPv6	✔	✔	✔	✔	La infraestructura de backup de Veeam está totalmente preparada para operar en los centros de datos modernos configurados con redes IPv6.
Cumplimiento FIPS	✔	✔	✔	✔	Los componentes de la infraestructura de respaldo de Veeam utilizan API y módulos criptográficos compatibles con FIPS.
Capacidad de auditoría	✔	✔	✔	✔	Realice un seguimiento de las acciones del usuario y las actividades de respaldo con eventos de auditoría y obtenga información valiosa sobre las operaciones de restauración a través de informes y alertas de auditoría específicos y flexibles.

©2022 Veeam Software. Todos los derechos reservados. Todas las demás marcas comerciales y logotipos son propiedad de sus respectivos dueños.

CONSORCIO EMDOC

Comparación de funciones de Veeam Data Platform

✔ Funciones incluidas ✔ Funcionalidad compatible

Opciones de licencias y compatibilidad Desarrollado por Veeam Copias de seguridad y replicación	Comunidad	Plataforma de datos de Veeam Licencia universal de Veeam (VUL) Base	Avanzado	Premium	Descripción
Backup					
Compatibilidad con hipervisores VMware vSphere y Microsoft Hyper-V	✔	✔	✔	✔	Proteja máquinas virtuales, datos, aplicaciones y más con la capacidad de recuperar inmediatamente cualquier elemento mediante una única copia de seguridad, además de una granular de elementos clave de la aplicación.
Compatibilidad con el hipervisor Proxmox VE	✔	✔	✔	✔	Protección de datos y recuperación granular para máquinas virtuales y datos de Proxmox VE con Proxmox VBR.
Compatibilidad con el hipervisor Nutanix AHV	✔	✔	✔	✔	Proteja las máquinas virtuales, los datos de aplicaciones y más gracias a la integración nativa con Nutanix AHV. Obtenga la capacidad de recuperar inmediatamente cualquier copia de seguridad o imagen de VM, además de realizar una recuperación granular de elementos clave de la aplicación.
Compatibilidad con Oracle Linux Virtualization Manager y el hipervisor Red Hat Virtualization	✔	✔	✔	✔	Protección de datos y recuperación granular para máquinas virtuales, datos y aplicaciones de Oracle Linux Virtualization Manager y el hipervisor Red Hat Virtualization.
Compatibilidad con IaaS y PaaS de nube pública	✔	✔	✔	✔	Opciones de instantáneas nativas, copias de seguridad basadas en snapshots y copias de seguridad basadas en agentes para máquinas virtuales alojadas en la nube, bases de datos, recursos compartidos de archivos y almacenamiento de objetos en proveedores líderes como Amazon Web Services (AWS), Microsoft Azure y Google Cloud.
Compatibilidad nativa con aplicaciones empresariales	✔	✔	✔	✔	Cree copias de seguridad coherentes con las aplicaciones con Microsoft SQL Server y Microsoft Exchange que tiene en cuenta las aplicaciones para lograr una recuperación granular. (La copia de seguridad del registro de transacciones para Oracle, PostgreSQL y SQL Server no está incluida en Community Edition).
Almacenamiento de objetos de nivel empresarial		✔	✔	✔	La solución de respaldo de confianza para la protección de las cargas de trabajo de MongoDB con copias de seguridad consistentes con las aplicaciones, integración nativa con herramientas de terceros y más.
Archivo empresarial	✔	✔	✔	✔	Proteja y archive recursos compartidos de archivos NAS (SMB y NFS) de manera eficaz y a escala. Realice copias de seguridad programadas en repositorios de Veeam para objetos de almacenamiento a corto y largo plazo. Los primeros 500 GB de archivo son completamente gratuitos con capacidad adicional con licencia VUL a 500 GB por licencia. Tecnologías de seguridad NAS en tiempo real, almacenamiento de objetos, cinta y más. La compatibilidad con el archivado de versiones de archivos no está disponible con la edición Community. Los primeros 500 GB de cualquier fuente de datos son gratuitos con licencia VUL a 500 GB por licencia.

CONSORCIO EMDOC
Documento Público

© 2024 Veeam Software. Todos los derechos reservados. Todas las marcas comerciales son propiedad de sus respectivos dueños.

Comparación de funciones de Veeam Data Platform

✔ Disponible incluido ✔ Disponible incluido

Copia de seguridad y recuperación *Desarrollado por Veeam* Calidad de seguridad y recuperación	Comunidad	Edición Universal de Veeam (VUL) Licencia universal de Veeam (VUL) Base	Avanzado	Premium	Descripción
Mejorado: Copia de seguridad del almacenamiento de objetos	✔	✔	✔	✔	Proteja los datos alojados en el almacenamiento de objetos con opciones de recuperación y copia de seguridad granulares. Capacidad de restauración diferencial tipo de almacenamiento de objetos (por ejemplo, de S3 a S3). Duplicar de copia de seguridad versión 10, incluyendo repositorios de copia de seguridad inmutables y con tiempo en general. Incluye nueva protección y resiliencia contra para los datos que residen en Azure Data Lake Storage Gen2. Los primeros 800 GB de cualquier fuente de datos son gratuitos con capacidad de carga con licencia VUL de 500 GB por hora.
Agentes *Para Microsoft Windows, Linux y macOS*	✔	✔	✔	✔	Copia de seguridad basada en agente para servidores y estaciones de trabajo Windows, Linux y macOS con implementación y gestión automatizadas directamente dentro de la consola de copia de seguridad.
Agentes de cifrado en la nube	✔	✔	✔	✔	Cree copias de seguridad que protejan los datos de aplicaciones de sus cargas de trabajo alojadas en máquinas virtuales de [illegible] con [illegible] con [illegible] agentes de Veeam específicos para la nube. Las características incluyen: a nivel de copia de seguridad directamente en el almacenamiento de objetos, el uso de los servicios de AWS, Microsoft Azure y Google Cloud para el equilibrio de carga de trabajo, y el funcionamiento independiente de una conectividad de red directa.
Agentes para AIX y Solaris		✔	✔	✔	Copia de seguridad basada en agente para servidores y estaciones de trabajo AIX y Solaris en repositorios de copia de seguridad de Veeam.
Trabajos de copia de seguridad	✔	✔	✔	✔	Cree automáticamente copias de seguridad a la ubicación de almacenamiento de respaldo [illegible] de la actividad y la recuperación para garantizar que los datos sean siempre protegidos.
Cifrado de extremo a extremo	✔	✔	✔	✔	Proteja los datos de respaldo y las transferencias de red con cifrado AES de 256 bits de extremo a extremo sin ningún impacto negativo en las tasas de reducción de datos de aceleración de WAN y compresión incorporadas. Todas las ediciones incluyen cifrado en origen, en tránsito y en reposo. La edición comunitaria no incluye protección contra contraseñas perdidas.
Orquestación de instantáneas primarias	✔	✔	✔	✔	Reduzca [illegible] de almacenamiento adicionales, aproveche [illegible] de seguridad del agente de instantáneas de Oracle y SQL Server en los nuevos dispositivos de almacenamiento principales para una amplia [illegible] de almacenamiento. La orquestación de instantáneas de almacenamiento secundario está disponible para [illegible] proveedores de almacenamiento.
Proxy con [illegible]		✔	✔	✔	Reduzca la carga en el servidor de respaldo central, mejore la escalabilidad y simplifique la red para entornos con una gran cantidad de oficinas remotas/sucursales (ROBO) al realizar el procesamiento consistente de la aplicación y la recuperación del sistema de archivos invitado.
Afinidad de proxy		✔	✔	✔	Evite el tráfico de red entre nodos en varios dispositivos Veeam todo en uno asociando servidores proxy y repositorios de respaldo ubicados en el mismo dispositivo.

CONSORCIO EMDOC

© 2024 Veeam Software. Todos los derechos reservados. Todas las marcas comerciales son propiedad de sus respectivos dueños.

117

Comparación de funciones de Veeam Data Platform

✔ Totalmente compatible ✔ Parcialmente compatible

Capacidad, seguridad y recuperación Datos protegidos por Veeam Copia de seguridad y replicación	Comunidad	Plataforma de datos de Veeam Licencia universal de Veeam (VUL) Básico	Avanzado	Premium	Descripción
Control de acceso de almacenamiento		✔	✔	✔	Establece el mantenimiento adaptable de la cuenta de S3 para los almacenes de datos de producción a fin de garantizar que las actividades de copia de seguridad y recuperación no afecten a la disponibilidad del almacenamiento para las cargas de trabajo de producción. La edición Premium incluye una configuración de resiliencia global.
Aceleración WAN incorporada		✔	✔	✔	Ofrenga varias y valiosas de copia de seguridad fuera del sitio para SO varias subscripciones y servicios de nube.
Copias de seguridad y copias de almacenamiento de procesamiento		✔	✔	✔	Crea copias de seguridad y réplica basadas en imágenes con la integración nativa de todas las principales proveedores de almacenamiento de nube para copias de seguridad a partir de instantáneas de almacenamiento primario y secundario. Esto incluye soporte para cada vez mayor métodos de autenticación y alianzas de empresa asignada.
Copia de seguridad y recuperación de nativa nube					
Copia de seguridad y recuperación de AWS	✔	✔	✔	✔	Protección nativa para Amazon EC2, Amazon RDS, Amazon Aurora, Amazon DynamoDB, Amazon S3, datos de Amazon VPC, Amazon FSx y Amazon Redshift. Opciones de restauración granular y de instancia completa disponibles en el lugar o como nuevas en la misma cuenta o región o en una diferente. Las opciones de copia de seguridad, restauración y migración fuera de AWS incluyen instalaciones locales, Microsoft Azure y Google Cloud.
Copia de seguridad y recuperación de Azure	✔	✔	✔	✔	Protección nativa para máquinas virtuales de Azure, Azure SQL, Azure Files, Azure Blob y Azure Cosmos DB. Opciones de restauración granular y de instancia completa disponibles en el lugar o como nuevas en la misma suscripción o región o en una diferente. Las opciones de copia de seguridad, restauración y migración fuera de Azure incluyen instalaciones locales, AWS y Google Cloud.
Copia de seguridad y recuperación en Google Cloud	✔	✔	✔	✔	Protección nativa para máquinas virtuales de Compute Engine, Cloud SQL para MySQL y PostgreSQL y Cloud Spanner. Opciones de restauración granular y de instancia completa disponibles en el lugar o como nuevas en el mismo proyecto o región o en una diferente. Las opciones de copia de seguridad, restauración y migración fuera de Google Cloud incluyen instalaciones locales, AWS y Microsoft Azure.
Control de DEVOPS	✔	✔	✔	✔	Operativo y compatible el patrón en la nube y, además, limpia cuenta con los objetivos de nivel de servicio, recepción y cumplimiento normativo. Las medidas de control de costes incluyen compresión de imágenes, deduplicación por niveles para cargas de almacenamiento de objetos de nivel, reporte avanzado de costes, previsión de consumo y planificación de capacidad.
Seguridad en la nube	✔	✔	✔	✔	Protege los datos de las copias de seguridad de acuerdo con las mejores prácticas y los marcos de trabajo de buena arquitectura. Las medidas de seguridad incluyen la separación física de las copias de seguridad, el acceso con privilegios mínimos mediante la gestión de identidades y accesos, la inspección con análisis de malware y gestión de claves propias para cifrados en tránsito y en reposo.

CONSORCIO ENDOC

Comparación de funciones de Veeam Data Platform

✔ Disponible en la edición ✔ Funcionalidad compatible

Copia de seguridad y recuperación *Desarrollado por Veeam* *Copia de seguridad y replicación*	Comunidad	Suscripción de Veeam Data Platform Licencia universal de Veeam (VUL) Básica	Avanzada	Premium	Descripción
Complementos y Protección de seguridad de aplicaciones empresariales					
Nuevo Complemento de Veeam para SAP HANA en IBM Power		✔	✔	✔	Elimine la necesidad de múltiples soluciones de respaldo en su centro de datos con el nuevo y potente complemento (disponible) certificado para SAP HANA que se ejecuta en IBM Power.
Nuevo Complemento de Veeam para IBM Db2 (Intel Linux y IBM AIX y IBM Power)		✔	✔	✔	Protege las bases de datos IBM Db2 que se ejecutan en Intel Linux, IBM AIX o IBM Power. Admite instancias independientes y recuperación ante desastres de alta disponibilidad (HADR)
Complemento de Veeam para Oracle RMAN, SAP HANA y SAP en Oracle		✔	✔	✔	Transmita copias de seguridad de Oracle RMAN, SAP HANA y SAP en Oracle a los repositorios de Veeam y recupérelas con facilidad, aprovechando las capacidades nativas de copia de seguridad y recuperación. Los complementos empresariales se pueden implementar en los sistemas operativos Linux, AIX, Solaris y Microsoft Windows. Incluye administración general en Windows y Linux.
Complemento de Veeam para Microsoft SQL		✔	✔	✔	Habilite las copias de seguridad nativas de Microsoft SQL Server directamente en los repositorios de almacenamiento de Veeam. La integración con Microsoft SQL Server Management Studio simplifica las tareas de administración de copias de seguridad y recuperación.
Almacenamiento de copias de seguridad					
Almacenamiento de objetos	✔	✔	✔	✔	Envíe copias de seguridad directamente al almacenamiento de objetos en las instalaciones o en la nube pública para una protección contra ransomware perimetral y para conservación a largo plazo. Compatibilidad con almacenamiento de objetos inmutable.
Repositorio reforzado de Linux	✔	✔	✔	✔	Mantenga sus copias de seguridad seguras en repositorios de Linux reforzados y a prueba de malware y ataques de fuerza bruta, con copias de seguridad inmutables que evitan el cifrado y la eliminación por parte de ransomware y actores malintencionados.
Copia de seguridad de Veeam Cloud Connect		✔	✔	✔	Realice sus copias de seguridad fuera de las instalaciones con una copia de seguridad totalmente integrada. Ubique, asegure y pruebe sus datos de forma segura en cualquiera de nuestros proveedores de servicios con tecnología Veeam. Una respuesta integrada frente al ransomware en la que cada copia de seguridad se transfiere a un repositorio externo, la ubicación de cada copia de seguridad se registra y todas las copias de seguridad directas en la nube.
Copia de seguridad de VMware Cloud Director	✔	✔	✔	✔	Realice copias de seguridad de vApps y archivos de vApp y VM, y restaure vApps y VMs directamente en vCloud con soporte completo para VMs con múltiples discos independientes. Todas las ediciones incluyen visibilidad integrada de la infraestructura en vCloud Director. Copia de seguridad a través de VeeamZIP incluida a copia de seguridad de metadatos y archivos de vApp y VM y restauración directa en vCloud. La Community Edition no incluye lo siguiente: soporte para trabajos de copia de seguridad avanzados programados de VMs de vCloud, integración del portal del cliente a través de API REST de, autoservicio, copia de seguridad y restauración de nivel de objeto por el inquilino a través de Enterprise Manager, así como asistencia comercial de vCloud Director.

Comparación de funciones de Veeam Data Platform

✔ [illegible] ✔ [illegible]

Capa de seguridad y recuperación *Desarrollado por Veeam* Copias de seguridad y replicación	Comunidades	Niveles de suscripción de Veeam Licencia Universal de Veeam (VUL) Básico	Avanzado	[illegible]	Descripción
Repositorio de respaldo escalable (SOBR) con soporte de almacenamiento de objetos		✔	✔	✔	Aproveche una capa de bloque adicional en los repositorios de almacenamiento existentes para crear un único grupo virtual de almacenamiento de respaldo para sus copias de seguridad. Use niveles de rendimiento, capacidad y archivo que automatizan la administración durante todo el ciclo de vida de las copias de seguridad. VUL se limita a dos escalas en cuanto a la cantidad de repositorios predeterminados.
Ampliación de capacidad de SOBR		✔	✔	✔	Aproveche la integración nativa del almacenamiento de objetos con AWS, Microsoft Azure, IBM Cloud, Google Cloud Storage y la mayoría de las plataformas de almacenamiento de objetos compatibles con S3 para repositorios locales o basados en la nube. Proteja sus copias de seguridad contra actividad malintencionada con la inmutabilidad basada en S3 Object Lock. Otras capacidades incluyen la capacidad de mover cadenas de copia de seguridad anteriores a la extensión de capacidad, copiar nuevos archivos de copia de seguridad, mover datos de la extensión de capacidad a las extensiones de rendimiento y restaurar datos del nivel de capacidad sin crear un nuevo SOBR.
Nivel de archivo SOBR		✔	✔	✔	Reduzca los costos de archivado y retención de datos a largo plazo hasta 20 veces y reemplace la administración manual de cintas con soporte nativo para Amazon S3 Glacier (incluido Glacier Deep Archive) y Microsoft Azure Archive Storage a través de la administración del ciclo de vida de respaldo de extremo a extremo.
Mejora del almacenamiento de objetos compatible con S3 con archivado de datos habilitado		✔	✔	✔	Vuelva los puntos de restauración [illegible] archivo de nuevo con [illegible] la API de almacenamiento de objetos inmutable para objetos compatibles con Amazon S3 Glacier.
Verificaciones de estado de almacenamiento de objetos		✔	✔	✔	Health Check verifica de forma proactiva la existencia de objetos mediante Execute API. Los proveedores de almacenamiento de objetos suelen tener una disponibilidad de 11 nueves. Health Check está diseñado [illegible]
Análisis de resiliencia [illegible]	✔	✔	✔	✔	[illegible] configuración de objetos de respaldo independientes para mejorar el rendimiento de copias de seguridad [illegible] copias de seguridad en dispositivos de almacenamiento de nivel empresarial y deduplicar dispositivos de almacenamiento. Esto se logra aprovechando el procesamiento paralelo de las máquinas virtuales para permitir múltiples flujos de entrada simultáneos.
Mover y copiar archivos de respaldo		✔	✔	✔	Mueva o copie archivos de respaldo en múltiples trabajos o repositorios para lograr fácilmente el nivel deseado [illegible] equilibrar el almacenamiento de respaldo o administrar escenarios de migración.
Compatibilidad [illegible]	✔	✔	✔	✔	Copia de seguridad de archivos en cualquier dispositivo de cinta compatible con LTO. Los trabajos de copia de seguridad de cinta preparan una [illegible] archivado más enfocado con encriptación de trabajos de copia de seguridad principales, un tipo de grupo de medios dedicado para simplificar la retención de GFS y grupos de medios globales para simplificar el uso de varios dispositivos de cinta. Compatibilidad con HDWORM para la protección de dispositivos [illegible] Soporte de VUL [illegible] para trabajos de archivo [illegible]

CONSORCIO EMDOC

[illegible] Todos los derechos reservados. Todas las demás marcas comerciales son propiedad de sus respectivos dueños.

Comparación de funciones de Veeam Data Platform

✔ [illegible] ✔ [illegible]

Capas de seguridad y recuperación Datos protegidos por Veeam Capas de seguridad y recuperación	Comunidad	Plataformas de datos de Veeam Licencia universal de Veeam (VUL) Básico	Avanzado	Premium	Descripción
Nexus Compatibilidad con [illegible]		✔	✔	✔	Reduce los costos sin comprometer la seguridad al combinar la protección de datos con espacio de aire de Veeam con almacenamiento de bajo costo a escala empresarial utilizando unidades IBM Jaguar
Repositorio externo de Veeam		✔	✔	✔	Conéctese a repositorios de almacenamiento de objetos administrados por capas de seguridad diseñados de la mano de Veeam, diferenciándose de las ofertas de seguridad de la competencia fuera de la nube para lograr el cumplimiento de la regla 3-2-1.
[illegible]		✔	✔	✔	[illegible]
Mejorado ONTAP de NetApp Soporte de FlexGroups	✔	✔	✔	✔	Habilite copias de seguridad y recupere grandes volúmenes en NetApp ONTAP FlexGroups para garantizar que sus datos no grandes estén protegidos a escala.
Compatibilidad con inmutabilidad de instantáneas primarias para HPE 3PAR/Primera/Alletra		✔	✔	✔	Compatibilidad con la creación de instantáneas inmutables en matrices HPE 3PAR/Primera/Alletra aprovechando la funcionalidad nativa de Virtual Lock. Se requiere una licencia válida de Virtual Lock.
[illegible]		✔	✔	✔	Permite la inmutabilidad y retención de copias de seguridad (GFS) mediante API REST de HPE StoreOnce Catalyst Copy.
Nuevas instantáneas para FlashCopies en IBM FlashSystem y el controlador de volumen SAN	✔	✔	✔	✔	Soporte para instantáneas de grupos de volúmenes (requiere IBM Spectrum Virtualize 8.5.1 o más reciente).
Mejorada inmutabilidad para Dell Data Domain con compatibilidad con bloqueo de retención nativo de DD		✔	✔	✔	Conserve sus copias de seguridad en el [illegible]
Nuevo [illegible]		✔	✔	✔	Capacidad de descubrir automáticamente el nodo del clúster que tiene el mejor volumen y procesamiento siempre que el almacenamiento se proporcione en clústeres compatibles nuevos.
[illegible]		✔	✔	✔	Obtenga un rendimiento de hasta [illegible] mejores copias de seguridad en integraciones de almacenamiento con deduplicación (Dell Data Domain Boost, HPE StoreOnce Catalyst, Quantum DXi y ExaGrid Accelerated DataMover).

[illegible]

4/21

Comparación de funciones de Veeam Data Platform

✔ Disponible y compatible ✔ Parcialmente compatible

Capa de seguridad y cifrado integrados desarrollados por Veeam Capa de seguridad y replicación	Comunidad	Plataforma de datos de Veeam: Licencia universal de Veeam (VUL) Base	Avanzado	Premium	Descripción
Replicación					
CDP de Veeam (Protección continua de datos)		✔	✔	✔	Elimine el tiempo de inactividad y el riesgo de pérdida de datos para las cargas de trabajo de nivel 1 de VMware vSphere y Cloud Director con CDP integrado y logre recuperaciones inmediatas a cualquier punto deseado en el tiempo, proporcionando los mejores objetivos de punto de recuperación (RPO).
NuevaSure Réplica para CDP		✔	✔	✔	Asegúrese de que la recuperación sea siempre operativa. La validación continua durante las pruebas de conmutación por error. Conmutación por error, archivos, objetos, Vista y verificación de CPC. Informes completos en Veeam Recovery Orchestrator.
Nueva funcionalidad en el nivel de archivo y protección para una réplica de CDP		✔	✔	✔	Vuelva atrás de la réplica de CDP desde cualquier punto de restauración, ¡incluso a nivel de archivo! Los bloques modificados antes de ransomware. La replicación continua garantiza que los cambios se reenvíen inmediatamente.
Recuperación nativa por error planificada con réplicas de CDP		✔	✔	✔	Recuperación verificada y probada para cuando necesita volver a la CONTINUIDAD. Orden de arranque de las cargas de trabajo.
[illegible]	✔	✔	✔	✔	[illegible]
[illegible]	✔	✔	✔	✔	Reversión de réplicas y conmutación por error y recuperación automática.
Replicación desde una copia de seguridad	✔	✔	✔	✔	Cree réplicas directamente desde archivos de respaldo sin afectar la producción
Replicación de Veeam Cloud Connect		✔	✔	✔	Garantice la disponibilidad de sus aplicaciones críticas con una recuperación ante desastres (DRaaS) con tecnología de Veeam. En caso de desastre o uso de prueba, las réplicas almacenadas en el repositorio se pueden utilizar para la conmutación por error parcial o total del sitio.
[illegible]		✔	✔	✔	Orquestación de pasos de recuperación que [illegible] con [illegible] para [illegible] el tiempo de inactividad y [illegible].
Replicación de VMware Cloud Director		✔	✔	✔	El tipo de trabajo de replicación dedicado permite a los proveedores de servicios realizar la replicación de vApp dentro y entre instancias de vCloud Director. El trabajo de replicación preserva las máquinas virtuales y los metadatos de vApp (como la ruta, el orden de inicio de las máquinas virtuales) para crear una réplica de vApp lista para usar en el vCloud Director de destino que se puede aprovechar al instante en caso de un desastre.

[illegible] Todas las marcas comerciales son propiedad de sus respectivos dueños.

08102024

M-22

Veeam

Comparativa de funciones de Veeam Data Platform

✔ Totalmente compatible ✔ Parcialmente compatible

Suite de seguridad y recuperación Desarrollado por Veeam Copia de seguridad y recuperación	Comunidad	Plataforma de datos de Veeam Licencia universal de Veeam (VUL) Base	Avanzado	Premium	Descripción
Restaurar					
[illegible]	✔	✔	✔	✔	Permitir a máquinas virtuales [illegible]
[illegible]	✔	✔	✔	✔	Restaure discos virtuales individuales y archivos específicos de VM (como VMDK) desde copias de seguridad y instantáneas de almacenamiento.
Restauración directa a AWS, Azure y Google Cloud	✔	✔	✔	✔	Restaure o migre máquinas virtuales, servidores físicos y puntos finales locales basados en Windows o Linux directamente a AWS, Microsoft Azure y Google Cloud.
Recuperación instantánea					
[illegible]	✔	✔	✔	✔	Acceda a copias de seguridad y réplicas con objetivos de tiempo de recuperación (RTO) casi de cero mediante la recuperación instantánea granular de máquinas virtuales, CLOUDLESS copia de seguridad y instantáneas en una [illegible] Microsoft Hyper-V o almacenamiento empresarial [illegible]
[illegible]	✔	✔	✔	✔	Publique [illegible] mediante [illegible] sin [illegible] en [illegible] en Veeam Backup & Replication (por ejemplo, con el disco [illegible]
[illegible]		✔	✔	✔	Recupere [illegible] cualquier base de datos de Microsoft SQL Server y Oracle desde una copia de seguridad al último estado o a un punto [illegible] a cualquier servidor o clúster de [illegible] de datos de producción físicos o virtuales [illegible] independientemente de su tamaño.
[illegible]	✔	✔	✔	✔	Restaure [illegible] archivos [illegible] de archivos [illegible] directamente [illegible] las copias de seguridad [illegible] con [illegible] [illegible] operativos [illegible] [illegible] y [illegible] [illegible] [illegible]

✔ Realmente completo ✔ Parcialmente completo

Copia de seguridad y recuperación *Desarrollado por Veeam* Copia de seguridad y replicación	Comunidad	Plataforma de datos de Veeam Licencia universal de Veeam (VUL)			Descripción
		Base	Avanzado	[illegible]	
Comparar con producción	✔	✔	✔	✔	Compara fácilmente los archivos de las copias de seguridad con el sistema de archivos de producción para ver y recuperarse solo los archivos modificados. Disponible solo para copias de seguridad a nivel de imagen. Community Edition y Standard solo pueden comparar y ver; VUL, enterprise y enterprise Plus pueden comparar, ver y restaurar a producción.
Recuperación de permisos		✔	✔	✔	Restaura los permisos perdidos o modificados de archivos [illegible]. Obligatorio para cumplir requisitos normativos y reducir riesgos.
NuevoVeeam Explorer para MongoDB		✔	✔	✔	Recuperación granular optimizada de colecciones, bases de datos e instancias de MongoDB sin necesidad de contar con un conjunto [illegible] de habilidades en MongoDB.
NuevoExplorador de Veeampara SAP HANA		✔	✔	✔	Restaure una sola base de datos o varias bases de datos desde las copias de seguridad del complemento SAP HANA con la calidad original y una interfaz [illegible] en cualquier momento y personalice las opciones de restauración.
NuevoExplorador de Veeampara PostgreSQLExplorar base de datos	✔	✔	✔	✔	Exporte bases de datos PostgreSQL específicas en el formato de volcado nativo directamente desde la copia de seguridad o desde la instancia PostgreSQL publicada.
Explorador de Veeampara Azure Blob Storage	✔	✔	✔	✔	Restaure objetos [illegible] de almacenamiento, [illegible] y elimine de [illegible] para cumplimiento de [illegible].
Explorador de Veeampara *PostgreSQL*	✔	✔	✔	✔	Restaure y publique instancias de PostgreSQL en el servidor original o en uno nuevo con facilidad, sin necesidad de conocimientos de administración de PostgreSQL. La recuperación de instancias de PostgreSQL está disponible con la edición Enterprise o superior.
Explorador de Veeampara *Microsoft Active Directory*	✔	✔	✔	✔	Búsqueda y restauración de todos los objetos de Active Directory (AD), como usuarios, grupos, cuentas de equipo y contactos, incluida la recuperación de contraseñas de usuario y equipo. Todas las ediciones admiten la restauración de cuentas de usuario y equipo individuales (incluida la capacidad de restablecer contraseñas), así como la exportación al formato LDIFDE. La Community Edition no permite la restauración de selección múltiple y la restauración de conexiones, la restauración de objetos de directiva de grupo (GPO) o la restauración de registros DNS integrados en AD y la restauración de objetos de partición de configuración.
Explorador de Veeampara *Microsoft Exchange*	✔	✔	✔	✔	Descarga visualizar [illegible] de las copias de seguridad de Microsoft Exchange para la recuperación de elementos individuales de Exchange (correos electrónicos, citas, notas, contactos, etc.), buzones de archivo en línea y elementos eliminados de forma permanente. Aproveche la funcionalidad integral de eDiscovery, que incluye la estimación del tamaño de los resultados de las consultas y los informes de exportación detallados. Community Edition no admite la restauración al buzón original.

CONSORCIO EMDOC Dominicano

© 2024 Veeam Software. Todos los derechos reservados. Todas las demás marcas comerciales son propiedad de sus respectivos dueños.

Comparación de funciones de Veeam Data Platform

✔ Funciones completas ✔ Presupuesto y limitados

Copias de seguridad y recuperación Desarrollado por Veeam Copias de seguridad y replicación	Comunidad	Plataforma de datos de Veeam Licencia universal de Veeam (VUL) Básico	Avanzado	[illegible]	Descripción
Explorador de Veeam para Microsoft SQL Server	✔	✔	✔	✔	Restaure bases de datos SQL individuales con facilidad, sin necesidad de tener conocimientos de SQL o tener que buscar archivos de bases de datos y registros de transacciones. Todas las ediciones admiten restauraciones de archivos de bases de datos SQL locales en un momento cronometrado. Sin embargo, Community Edition no incluye copias de seguridad y reproducción de registros de transacciones. Si agrega [illegible] nivel de granularidad de bases de datos y objetos SQL aislados, procedimientos almacenados, vistas, etc.) en el servidor SQL original en el nivel.
Explorador de Veeam para Microsoft SharePoint	✔	✔	✔	✔	Obtenga visibilidad total y [illegible] de las copias de seguridad de SharePoint con funciones avanzadas de búsqueda y exploración para recuperar rápidamente elementos individuales de SharePoint y sitios completos. Todas las ediciones admiten la restauración de elementos de SharePoint mediante la función de guardar, enviar y exportar. Sin embargo, Community Edition no agrega la restauración de sitios completos ni la restauración a la ubicación original.
Nombre del explorador de Veeam para PostgreSQL (disponibilidad limitada)		✔	✔	✔	Proporcione disponibilidad instantánea a PostgreSQL directamente desde su copia de seguridad, sin comprometer la recuperación y el registro de datos en segundo plano.
[illegible]	✔	✔	✔	✔	Un catálogo de archivos creados que permite realizar búsquedas sencillas en archivos creados para encontrar y recuperar un archivo en cualquier momento en que se necesite. Todas las ediciones proporcionan un catálogo de archivos limitado en las copias de seguridad que se encuentran actualmente en disco. La Community Edition no proporciona un catálogo de archivos de copia de seguridad archivados fuera de línea con el clic para habilitar recuperaciones directamente desde los equipos de biblioteca.
Explorador de Veeam para Oracle		✔	✔	✔	Restaure bases de datos Oracle individuales con facilidad, sin necesidad de tener conocimientos profundos de Oracle o de buscar archivos de bases de datos y registros de transacciones. Incluya copia de seguridad de registros de transacciones sin agentes, administración de registros archivados y recuperación de bases de datos a nivel de transacciones en el servidor Oracle original o nuevo, así como la capacidad de publicar y exportar bases de datos Oracle.
Inmutabilidad de datos					
Restauración segura		✔	✔	✔	Aumente la seguridad y reduzca las interrupciones causadas por virus y ransomware con un paso de restauración seguro y sin riesgos mediante un análisis antivirus opcional de archivos de respaldo antes de la recuperación; soporte independiente para Windows Defender, ESET, Kaspersky y Symantec Protection Engine, así como la capacidad de extenderse a otras herramientas antivirus y de hash con IO. El análisis YARA no está disponible en Community y Foundation.
[illegible]		✔	✔	✔	Incluya y verifique automáticamente la capacidad de recuperación de cada copia de seguridad ejecutando automáticamente pruebas de recuperación de máquinas virtuales en un entorno aislado de su elección, con [illegible] y [illegible] en la lista de verificación de aplicaciones personalizadas. Los análisis de YARA no están disponibles en Community Edition y Foundation.

CONSORCIO EMOC

Comparación de funciones de Veeam Data Platform

✔ Versiones completas ✔ Funcionalidad completa

Copia de seguridad y replicación *Desarrollado por Veeam* *Copia de seguridad y replicación*	Comunidad	Plataforma de datos de Veeam Licencia universal de Veeam (VUL)			Descripción
		Base	Avanzado	Premium	
Réplica segura		✔	✔	✔	Pruebe y verifique automáticamente la capacidad de recuperación de cada réplica realizando una conmutación por error a una ruta protegida de su entorno de producción, incluido soporte para scripts de prueba de aplicaciones personalizados.
Restauración por etapas		✔	✔	✔	Limpie los datos confidenciales del punto de restauración seleccionado de una copia aislada de su entorno de producción antes de restaurar el estado modificado de la máquina virtual a producción.
Sandbox a pedido[4]		✔	✔	✔	Ejecute una o más máquinas virtuales directamente desde una copia de respaldo cercada de su entorno de producción para solucionar problemas, probar actualizaciones y capacitar al personal en una copia de trabajo del entorno de producción, sin afectar las operaciones comerciales.
Sandbox a pedido desde instantáneas de almacenamiento[7]		✔	✔	✔	Utilice instantáneas de almacenamiento para crear rápidamente copias de trabajo de su entorno de producción que funcionen con el mismo rendimiento de E/S.
API de integración de datos		✔	✔	✔	Monte sus copias de seguridad inmutables en cualquier lugar. Ponga sus datos de seguridad a trabajar y rescate sus datos al ataque que aprovechan los errores humanos eliminando la dependencia de cualquier copia de seguridad de Veeam para recuperar datos. Análisis de seguridad, comprobaciones de cumplimiento y otros escenarios de reutilización de datos.
Autoservicio					
Portal de autoservicio de archivos y objetos para restauraciones por los propietarios de aplicaciones		✔	✔	✔	Restaure archivos, objetos y discos duros virtuales con un solo clic a través de una interfaz web.
Portal de recuperación de elementos de Microsoft Exchange para operadores de soporte técnico		✔	✔	✔	Restaure los elementos faltantes del buzón de correo al buzón original con un solo clic a través de una interfaz de usuario web.
Portal de recuperación de bases de datos de Microsoft SQL Server para operadores de soporte técnico		✔	✔	✔	Restaure bases de datos individuales al servidor original o a un nuevo servidor SQL con un solo clic a través de una interfaz de usuario web.
Portal de recuperación de bases de datos para Oracle y PostgreSQL		✔	✔	✔	Restaure bases de datos Oracle en el servidor original, un nuevo servidor Oracle o PostgreSQL con un solo clic a través de una interfaz de usuario web.
Portal de recuperación de archivos para operadores de soporte técnico		✔	✔	✔	Portal de restauración de archivos con salida de autoservicio en máquinas Linux y delegación automatizada según la membresía del grupo de administradores locales.

COPIA CONTROLADA
COPIA NO CONTROLADA

Los términos y condiciones de Veeam se aplican a todos los documentos mencionados. Consulte la información completa sobre las limitaciones y responsabilidades.

✔ Todavía no compatible ✔ Parcialmente compatible

Gestión de portabilidad y flexibilidad de datos Desarrollado por Veeam Copia de seguridad y replicación	Comunidad	Plataforma de datos de Veeam Licencia universal de Veeam (VUL) Básica	Avanzado	Premium	Descripción
Delegación de restauración		✔	✔	✔	Habilita a autoservicio usuarios seguros de restauración de archivos web, aplicaciones y equipos de VM para restauraciones de archivos y aplicaciones específicas, como Active Directory, Microsoft SQL Server, Oracle y más.
Complemento nativo de VMware Cloud Director		✔	✔	✔	Esta capacidad permite a los proveedores de servicios ampliar la interfaz de usuario de vCloud Director para incluir la funcionalidad de Veeam Backup & Replication, lo que permite a los usuarios gestionar sus propias copias de seguridad y restauraciones sin abandonar la comodidad de la consola web de vCloud Director. Esta integración se basa en el portal de autoservicio de copias de seguridad y restauración de vCloud Director existente de Veeam.
Control de acceso basado en roles (RBAC)		✔	✔	✔	Permite que los propios administradores y auditores de forma segura las copias de seguridad y recuperaciones de sus propias máquinas virtuales a través del portal de copia de seguridad y recuperación de autoservicio para vSphere con capacidades de delegación de restauración granulares, como archivos, aplicaciones, unidades de disco virtual y máquina virtual completa.
Gestión					
Veeam Backup Enterprise Manager: interfaz web de gestión centralizada		✔	✔	✔	Acceso a una vista consolidada basada en la Web de su implementación distribuida en un único panel que incluye autenticación centralizada, generación de informes, alertas centralizadas en varios servidores de respaldo y la capacidad de ejecutar y detener trabajos. Además, cuenta con una funcionalidad completa de gestión de trabajos y la capacidad de realizar restauraciones, incluida la restauración instantánea para VMware, Hyper-V, copias de seguridad de NAS, así como la migración a producción.
Módulo de PowerShell	✔	✔	✔	✔	Utiliza los cmdlets de PowerShell para crear flujos de trabajo personalizados y automatizar las tareas de Veeam.
API RESTful		✔	✔	✔	Integre los sistemas existentes y ejecute y automatice las tareas de Veeam mediante almacén de API RESTful. Los proveedores de servicios que utilizan licencias de alquiler tienen acceso a la API en todas las ediciones.
Gestión integrada para agentes de Veeam	✔	✔	✔	✔	La capacidad de organizar, automatizar e implementar agentes en Windows, Linux, Mac, AIX y Solaris con grupos de protección basados en contenedores de Active Directory, archivos CSV o etiquetas de nube pública para configurar actualizaciones automáticas personalizadas y protección de implementación. La Community Edition está limitada a 10 instancias.
Gestión integrada para [illegible] de Veeam		✔	✔	✔	Simplifique las operaciones con capacidades de administración centralizada para organizar, automatizar e implementar complementos de bases de datos Oracle RMAN, SAP HANA y SAP en Oracle, incluida la creación de políticas de [illegible] aplicaciones.

[illegible] VMware [illegible] Microsoft Hyper-V

[illegible] Veeam Software. [illegible] Todos los derechos reservados. Todas las demás marcas comerciales son propiedad de sus respectivos dueños.

Comparación de suscripciones de Veeam Data Platform

✔ Totalmente compatible ✔ Parcialmente compatible

Monitoreo y análisis *Desarrollado por Veeam ONE*	Plataforma de datos de Veeam			Descripción
	Comunidad	Avanzado	[illegible]	
Registro en línea y presentación de informes				
Nuevo Panel de control de Veeam Threat Center		✔	✔	Resalte amenazas, identifique riesgos y mida el nivel de seguridad de su entorno desde un único panel. Análisis centralizado para toda la plataforma.
Nueva integración de ServiceNow	✔	✔	✔	Cicle de vida de incidentes bidireccional con ServiceNow. Las anomalías de respaldo se informan automáticamente a ServiceNow para que pueda realizar una clasificación de inmediato y reduce aún más el riesgo para sus datos.
Mejoras administrativas de la plataforma		✔	✔	Monitoreo completo, informes y alarmas para nuevas funcionalidades, incluyendo: Backup de almacenamiento de objetos, motor de detección de malware y analizador de seguridad y cumplimiento.
Monitoreo del rendimiento y alertas para la actividad de respaldo	✔	✔	✔	La supervisión del rendimiento y las alertas de la actividad de copia de seguridad incluyen los trabajos de Veeam Backup & Replication, incluido su estado más reciente y las estadísticas de rendimiento. Veeam ONE no tiene limitaciones en la cantidad de servidores de Veeam Backup & Replication que se pueden supervisar. Tenga en cuenta que Veeam ONE Monitor [illegible]
Visualización e informes sobre alarmas		✔	✔	Reciba notificaciones de alarma a través de un correo electrónico para [illegible]
Informes generales de Veeam Backup	✔	✔	✔	Veeam ONE incluye varios informes, entre ellos descripciones generales de las configuraciones de Veeam Backup & Replication, auditorías de infraestructura de respaldo, informes de cumplimiento, máquinas virtuales (VM) protegidas, planificación de capacidad, informes de cinta y más.
Protección contra malware *para Nutanix AHV*	✔	✔	✔	Soporte para Veeam Backup para Nutanix AHV incluye varias alarmas e informes que le ayudan a analizar tendencias y determinar cómo han evolucionado las políticas y los trabajos de respaldo, así como a determinar el estado de respaldo de las máquinas virtuales de Nutanix. Esto ayuda a los usuarios a verificar el estado de protección de datos de cada máquina virtual detectada según el acuerdo de nivel de servicio (SLA) acordado.
Veeam Backup para Proxmox VE y oVirt KVM	✔	✔	✔	La compatibilidad con Veeam Backup para Proxmox VE y oVirt KVM incluye varias alarmas e informes que le ayudan a analizar tendencias y determinar cómo han evolucionado las políticas y los trabajos de backup, así como a determinar el estado de backup de las cargas de trabajo que se ejecutan en estas plataformas. Esto ayuda a los usuarios a verificar el estado de protección de datos de cada máquina virtual detectada en función del acuerdo de nivel de servicio (SLA) acordado.
Alarmas y generación de informes de Veeam agent	✔	✔	✔	El soporte para agentes de backup de Veeam incluye varias alarmas e informes que le ayudan a analizar tendencias y determinar cómo han evolucionado las políticas y los trabajos de backup, así como determinar el estado del backup de los agentes, incluidos los agentes que no tienen copias de backup y cuántos están protegidos o desprotegidos. Esto se proporciona con el estado del backup junto con la cantidad total de éxitos, advertencias y errores.

CONSULTADO EMDOC

[illegible] Todos los derechos reservados. [illegible]

Comparación de funciones de Veeam Data Platform

✔ Disponible completo ✔ Disponible parcial

Monitoreo y análisis *Desarrollado por Veeam ONE*	Plataforma de datos de Veeam			Descripción
	Comunidad	Avanzado	[illegible]	
Informes de Veeam Cloud Connect	✔	✔	✔	Los informes incluyen información sobre la infraestructura de Veeam Cloud Connect, como el uso de la puerta de enlace, la planificación de la capacidad para los repositorios en la nube y los datos de configuración para los repositorios y los puentes de salto en la nube.
Monitoreo y alertas de rendimiento para Veeam Cloud Connect	✔	✔	✔	La supervisión y alertas de rendimiento para Veeam Cloud Connect muestra trabajos solo para servidores de backup de Veeam Cloud Connect, incluido su estado más reciente y estadísticas de rendimiento. Hoja: Para supervisar y generar informes sobre clientes administrados, Veeam ONE debe implementarse en el sitio del inquilino. Veeam ONE *Edición comunitaria* está limitado a una versión de evaluación.
Mapas de calor	✔	✔	✔	Los mapas de calor ayudan a planificar el uso de los recursos y optimizar finalmente las actividades de backup con visibilidad en tiempo real de los repositorios de backup y servidores proxy. Veeam ONE *Edición comunitaria* está limitado a tres servidores proxy y tres repositorios.
Monitoreo y alertas para la nube híbrida				
Copia de seguridad de Veeam para AWS, Copia de seguridad de Veeam para Microsoft Azure y Veeam Backup para Google Cloud— Soporte nativo de protección de datos	✔	✔	✔	Monitoreo y alertas: los usuarios de Veeam ONE ahora pueden monitorear el estado de los trabajos de backup y estado de inactividad de cargas de trabajo basadas en la nube a través de alarmas y notificaciones predefinidas. Informes de estado de backup, inventario de máquinas virtuales protegidas predefinido ahora incluye máquinas virtuales alojadas en nubes públicas de AWS, Microsoft Azure y Google Cloud Platform. Esto ayuda a los usuarios a verificar el estado de protección de datos de cada máquina virtual de nube, según el acuerdo de nivel de servicio (SLA) acordado.
Informes	✔	✔	✔	Obtén una visibilidad detallada de los servicios protegidos y no protegidos de cualquier nube pública. Compatible con AWS (EC2, RDS, EFS, VPC), Microsoft Azure (máquinas virtuales, base de datos SQL, archivos de Azure) y Google Cloud Platform (Compute Engine, Cloud SQL).
Alarmas para violación de protección de datos en tiempo real	✔	✔	✔	Para cargas de trabajo en la nube protegidas por Veeam ONE Client, máquinas virtuales, bases de datos, VPC y recursos compartidos de archivos. Además del estado y la fecha de la última copia de seguridad, se han incorporado la última copia de seguridad y el último archivo para una visibilidad completa de la recuperación de datos.
Monitoreo y alertas para infraestructura virtual				
Monitoreo y alertas de rendimiento para infraestructura virtual	✔	✔	✔	Vistas de hosts de infraestructura virtual, almacenes de datos y clústeres. En Veeam ONE *Edición comunitaria*, los gráficos de rendimiento solo muestran una semana de rendimiento y los correos electrónicos incluyen detalles de alarma limitados.
Supervisión y gestión a nivel de aplicación	✔	✔	✔	Garantice la disponibilidad de aplicaciones críticas, monitoree grupos selectos de aplicaciones y cree alarmas adicionales para monitorear los estados de servicio de las máquinas virtuales. Asegúrese de que los procesos no excedan los recursos disponibles, identifique si se han deshabilitado aplicaciones críticas, como software antivirus, o indique si se han realizado cambios no deseados. Con Veeam ONE *Edición comunitaria* puede supervisar una cantidad limitada de aplicaciones en hasta tres máquinas virtuales.

[illegible] 08292024

CONSORCIO EMDOC

✔ Incluido en la edición ✔ Funcionalidad compatible

Monitoreo y análisis *Desarrollado por Veeam ONE*	Plataforma de datos de Veeam			Descripción
	Conectividad	Avanzado	Premium	
Informes de VMware vSphere y Microsoft Hyper-V	✔	✔	✔	Los paquetes de informes incluidos para vSphere y Hyper-V proporcionan comprobaciones completas de la configuración de servidores vCenter, almacenes de datos, clústeres, hosts y recursos virtuales, así como SDDC, volúmenes, clústeres, hosts y máquinas virtuales, incluida información sobre las alarmas más comunes generadas para objetos de infraestructura virtual. Los paquetes de informes de optimización también permiten a los usuarios evaluar la utilización de datos de recursos y optimizar el aprovisionamiento de recursos de máquinas virtuales para ayudar a lograr un mejor resultado y un mayor retorno de la inversión para entornos virtualizados. Con Veeam ONE Editión convencional, los informes de optimización están limitados a 10 000 de sus máquinas virtuales y los informes de rendimiento histórico están limitados a las últimas 24 horas de datos.
Informes y supervisión de múltiples inquilinos	✔	✔	✔	Obtener informes a los administradores del estado sobre un alcance limitado de máquinas virtuales organizadas por dominio vSphere.
Evaluación de infraestructura Veeam Backup & Replication	✔	✔	✔	Los informes de evaluación están diseñados para verificar que la implementación de Veeam Backup & Replication cumple con todas las mejores prácticas conocidas
Evaluación de infraestructura virtual	✔	✔	✔	Los informes de evaluación están diseñados para verificar que su infraestructura VMware vSphere y/o Microsoft Hyper-V cumple con todas las mejores prácticas conocidas.
Supervisión y alertas de VMware Cloud Director	✔	✔	✔	Las empresas quieren mantenerse a la vanguardia de los problemas que afectan a sus centros de datos virtuales y, en última instancia, a sus clientes. Para ayudar, Veeam ofrece capacidades para proporcionar a los equipos de proveedores de servicios en la nube un seguimiento de la disponibilidad y la configuración de sus centros de datos virtuales, incluidas las organizaciones y los vApps.
Informes de VMware Cloud Director	✔	✔	✔	Las empresas quieren asegurarse de utilizar la configuración ideal y optimizar sus recursos para aprovechar al máximo su infraestructura virtual al construir y mantener centros de datos virtuales para brindar un servicio confiable a sus clientes
Personalización y automatización de informes y alarmas				
Análisis detallado en grupo		✔	✔	Cree informes personalizados de Microsoft Excel utilizando las plantillas que usted defina.
Plantillas de informes predefinidas y personalizables	✔	✔	✔	Personalice y guarde plantillas de informes predefinidas para crear informes que se ajusten a sus necesidades específicas de información y formato. Veeam ONE Editión convencional se limita a guardar una plantilla de informe personalizada.
Generación y entrega de informes programados		✔	✔	Programe informes para que se generen automáticamente y se envíen a su bandeja de entrada, panel de control, portales web o archivos.
Escalamiento y manejo de alarmas	✔	✔	✔	Asegúrese de tener una cobertura de monitoreo completa mediante la creación de alarmas personalizadas para eventos exclusivos de su entorno virtual. Modele las alarmas en función de los datos de rendimiento anteriores para comprender la frecuencia potencial de las alarmas y evitar comentarios de alertas irrelevantes y eventos no detectados.

CONSORCIO EMDOC

Comparación de funciones de Veeam Data Platform

✔ Incluido en el plan ✔ Disponible como complemento

Monitoreo y análisis *Desarrollado por Veeam ONE*	Plataforma de datos de Veeam			Descripción
	Gratuito	Avanzado	Premium	
Gobernanza y cumplimiento				
Visión empresarial	✔	✔	✔	Clasifique y agrupe cargas de trabajo, máquinas virtuales y almacenes de datos por criterios como unidades de negocio, departamento, propósito y SLA. Aproveche VMware Tags para ayudar con el control de acceso basado en roles y eleve el nivel de seguridad, incluso el requisito de mantener confidencialidad por obligación para cumplir con el cumplimiento. Supervise fácilmente las aplicaciones independientemente de la ubicación geográfica, y establezca los objetos de la vista empresarial en función de múltiples parámetros para recopilar información sobre cómo se aprovechan los inversionistas en infraestructura. También puede asignar administradores para que administren parámetros específicos.
Automatización inteligente				
Diagnóstico inteligente de Veeam	✔	✔	✔	Identificación y alerta proactivas de problemas conocidos dentro de su entorno Veeam, lo que proporciona soluciones de autoayuda mediante revisiones o reconfiguraciones. Para Veeam ONE *Edición comunitaria* todas las alarmas seguirán funcionando, pero no se mostrarán los detalles de cada una.
Acciones de remediación	✔	✔	✔	La resolución predefinida y automatizada de problemas comunes relacionados con las copias de seguridad y la infraestructura virtual con acciones de reparación automáticas ayuda a reducir los costos de administración de TI. Con Veeam ONE *Edición comunitaria* hay acciones de remediación disponibles, pero requieren aprobación manual
Paneles de control				
Paneles de rendimiento predefinidos para infraestructuras virtuales y de respaldo y Veeam Backup para Microsoft 365	✔	✔	✔	Obtenga vistas rápidas de los trabajos de respaldo y la infraestructura de respaldo, así como una categorización amplia, los hosts y los clústeres que son los mayores consumidores de recursos de CPU, memoria, rendimiento de disco. Además, realice métricas de operaciones de almacenamiento de datos, incluidas las métricas relacionadas con las instantáneas de las máquinas virtuales y el uso del espacio en el almacenamiento
Paneles de informes personalizados	✔	✔	✔	Cree sus propias vistas rápidas de su entorno virtual. Veeam ONE *Edición comunitaria* permite crear un panel de informes personalizado
Planificación de capacidad				
Planificación de la capacidad VMware vSphere y Microsoft Hyper-V		✔	✔	Los paquetes de informes individuales para VMware vSphere y Microsoft Hyper-V están diseñados para pronosticar cuándo los recursos de infraestructura virtual disponibles alcanzarán sus niveles mínimos. Los paquetes brindan recomendaciones sobre la asignación de recursos y el equilibrio de carga para optimizar el rendimiento y la utilización de recursos en su respectivo entorno virtual y evitar posibles cuellos de botella en el rendimiento

CONSORCIO EMDOC

✔ Totalmente compatible ✔ Parcialmente compatible

Monitoreo y análisis *Desarrollado por Veeam ONE*	Plataforma de Veeam Data			Descripción
	Comunidad	Avanzado	Premium	
Inventario y mapeo de infraestructura		✔	✔	Aproveche escenarios de modelado hipotéticos totalmente automatizados para agregar o eliminar de forma segura máquinas virtuales o hosts de su infraestructura y calcular con precisión los recursos necesarios para cada proyecto.
Contracargo y facturación				
Informes de análisis de contracargos		✔	✔	Los informes de contracargos le ayudan a comprender los costos asociados con los usuarios individuales de la infraestructura virtual, así como realizar contracargos mediante el análisis de la configuración de la máquina virtual y el uso de recursos, incluidos la CPU, la memoria y el almacenamiento. Se incluyen cuatro informes: contracargo por configuración del host, contracargo por uso de recursos del host, contracargo por configuración de la máquina virtual y contracargo por rendimiento de la máquina virtual.
[illegible]	✔	✔	✔	Este informe proporciona capacidades de contracargo para Veeam Backup & Replication y ayuda a evaluar los costos de administración de almacenamiento para operaciones de respaldo y replicación, proporcionando datos que puedan utilizarse en informes financieros y de facturación.

CONSORCIO EMDOC
SANTA CATALINA D.C.

[illegible] Todos los derechos reservados. Todas las marcas comerciales son propiedad de sus respectivos dueños.

Comparación de funciones de Veeam Data Platform

✔ Funciones compatibles ✔ Funciones completas

Orquestación de recuperación *Desarrollado por Veeam Recovery Orchestrator*	Disponible en la edición de Veeam	Descripción
Orquestación y automatización de la recuperación		
Nuevo Gestión de reglas de YARA	✔	Los archivos de reglas de Yara se pueden importar a VBO, lo que permite una mayor seguridad, capacidad de administración y estabilidad. Combine las definiciones de reglas a diferentes grupos mediante los ámbitos de VBO y comprueba si hay presencia de contenido de las reglas de Yara en la cuenta de usuario de VBO, lo que permite el control de versiones y otras ventajas. Con la distribución automatizada, los archivos de Yara se envían de forma segura a los servidores de Veeam backup, se utilizan para el análisis y luego se eliminan.
Nuevo Soporte para repositorios adicionales	✔	Recuperación de Veeam Data Cloud Vault y repositorios S3: AWS, Wasabi, S3 local
Mejorado Recuperación de limpieza automatizada	✔	Los puntos de restauración que se marcaron como limpios durante la copia de seguridad pueden usarse para recuperación progresiva de todo un sistema mediante pruebas de restauración limpias de malware
Mejorado Pruebas para planes de réplica de CDP	✔	Pruebas de réplica de CDP sin impacto en la producción o la replicación. Pruebas con ejecuciones, comprobaciones de salida, pruebas de valor arbitrario personalizadas, modos de funciones de generación de informes de VBO habilitados.
Nuevo Soporte virtual con Microsoft Azure	✔	Reduzca el tiempo de inactividad y elimine los errores manuales al recuperar sus cargas de trabajo virtuales en Microsoft Azure empleando la configuración y validación del dominio operativo para crear la recuperación, leyendo varios puntos de restauración en formato nativo del hipervisor desde el repositorio de copias de seguridad de agente o vSphere y con todos los resultados de los scripts ejecutados en máquinas de VBO.
Recuperación masiva con casos de clic	✔	Permite que los propietarios de aplicaciones recuperen de forma segura aplicaciones individuales o pilas complejas con un clic. Ejecute planes de recuperación ante desastres para equipos de recuperación autoservicio a gran escala.
Recuperación en la nube	✔	La restauración directa compatible con Azure le brinda la oportunidad de una mayor flexibilidad con la recuperación ante desastres en la nube. Organice la recuperación de cualquier copia de seguridad como una máquina virtual en Azure, con mapeo automatizado de recursos de máquinas virtuales y redes en la nube.
Nuevo Análisis de malware	✔	Durante la recuperación realice escaneos automáticos de varios puntos de restauración para encontrar el más reciente que esté limpio. Analice periódicamente los puntos de restauración durante las pruebas de DataLab y muestre los resultados en paneles e informes para mejorar la visibilidad.
Mejorado Simulación de DataLabs	✔	Las pruebas de DataLabs simulan los resultados de la recuperación ante desastres, con pruebas de recuperación ante desastres totalmente automatizadas en una sola tarea sin afectar los sistemas de producción, y envían informes detallados. Cree y programe DataLabs para permitir que los equipos de aplicaciones apliquen actualizaciones, parches y más de manera segura.
Mejorado RBAC y delegación	✔	Divida las tareas y roles de recuperación relacionados con cuentas personalizadas, permita a los administradores un control total sobre el proceso de recuperación, limite permisos y delegue responsabilidades específicas a equipos especializados y descargue a los administradores de respaldo.

Copyright © 2024 Veeam Software. Todos los derechos reservados. Todas las marcas comerciales son propiedad de sus respectivos dueños.

Comparación de funciones de Veeam Data Platform

✔ Totalmente cumplido ✔ Parcialmente cumplido

Orquestación de recuperación *Desarrollado por Veeam Recovery Orchestrator*	Plataforma de datos de Veeam	Descripción
Pruebas de aislamiento y garantías de ciberseguridad		
Documentación dinámica	✔	Los informes se generan automáticamente para las definiciones, comprobaciones, pruebas y ejecuciones de planes de orquestación. Estos informes eliminan la carga de producción de documentación detallada y simplifican la auditoría. La documentación se produce en dos formatos, con detalles completos para un análisis profundo y un resumen ejecutivo.
Monitoreo del cumplimiento para RTO y RPO	✔	Los informes se generan automáticamente para las definiciones, comprobaciones, pruebas y ejecuciones de planes de orquestación. Estos informes eliminan la carga de producción de documentación detallada y simplifican la auditoría. La documentación se produce en dos formatos, con detalles completos para un análisis profundo y un resumen ejecutivo.
Controles de preparación programados	✔	Los informes se generan automáticamente para las definiciones, comprobaciones, pruebas y ejecuciones de planes de orquestación. Estos informes eliminan la carga de producción de documentación detallada y simplifican la auditoría. La documentación se produce en dos formatos, con detalles completos para un análisis profundo y un resumen ejecutivo.
Auditoría del plan DR	✔	El seguimiento cuantificado de los controles del plan de DR, registrado con marca de tiempo y nombre de usuario, permite un análisis detallado del historial del plan.

CONSORCIO EMDOC

Traducido del inglés al español - www.onlinedoctranslator.com

VEEAM

Producto

PLATAFORMA DE DATOS VEEAM: RESPALDO Y RECUPERACIÓN

Copia de seguridad y replicación de Veeam

Posea, controle, respalde y recupere todos sus datos, en cualquier lugar de la nube híbrida

Desafío

Muchos equipos de TI empresariales se confían en sus estrategias de protección de datos debido a la ineficiencia de las copias de seguridad heredadas, las recuperaciones poco confiables y las complejas administración en todo su centro de datos.

Veeam Copia de seguridad y replicación es la solución de respaldo, recuperación y seguridad de datos líder en el mundo para todas sus cargas de trabajo, tanto en las instalaciones como en la nube. Como componente fundamental de Veeam Data Platform, Veeam Backup & Replication ofrece una protección de datos segura, potente y confiable. Elimine el tiempo de inactividad con Instant Recovery y manténgase a salvo de las amenazas cibernéticas con inmutabilidad nativa y copias de seguridad probadas. Todo desde una consola diseñada por software e independiente del hardware.

- Cumpla con los objetivos de recuperación con confianza
- Reduzca el riesgo con una seguridad de datos integral
- Acelere su paso a la nube híbrida

Los apagones son más comunes de lo que piensas

✔ 53% de ellos de ciberseguridad

✔ 52% infraestructura o redes

✔ 49% borrado accidental

✔ 53% aplicaciones

Capacidades clave

Amplia protección

Asegure sus copias de seguridad locales en entornos de nube, virtuales, físicos y NAS.

Recuperación flexible

Logre sus acuerdos de nivel de servicio (SLA) con rápidas acciones confiables de alcance de la recuperación instantánea.

Agentes integrados en la nube

Copias de seguridad y recuperación con plataformas de AWS, Microsoft Azure y Google Cloud

Libertad de elección

Soluciones 100% definidas por software y agnósticas de hardware para máxima flexibilidad.

Seguridad integrada

Cree copias de seguridad inmutables para los ataques cibernéticos con cualquier dispositivo de almacenamiento de confianza.

Portabilidad de datos

Restaure en múltiples nubes y plataformas en un formato de datos portátil.

Seguridad en la nube

Utilice AWS KMS, Azure Key Vault, la inmutabilidad y más para evitar ataques de ransomware

Recuperación confiable

Las pruebas automatizadas de copias de seguridad y réplicas garantizan la recuperación.

Escale con facilidad

Reduzca los costos de almacenamiento de objetos mediante niveles inteligentes para mejorar la eficiencia de su presupuesto de la nube.

Alcance

Obtenga una cobertura de copia de seguridad nativa para una amplia gama de cargas de trabajo, incluidas máquinas virtuales (VM), bases de datos y más.

Proteja la infraestructura

La verificación automatizada de la recuperación garantiza la recuperación.

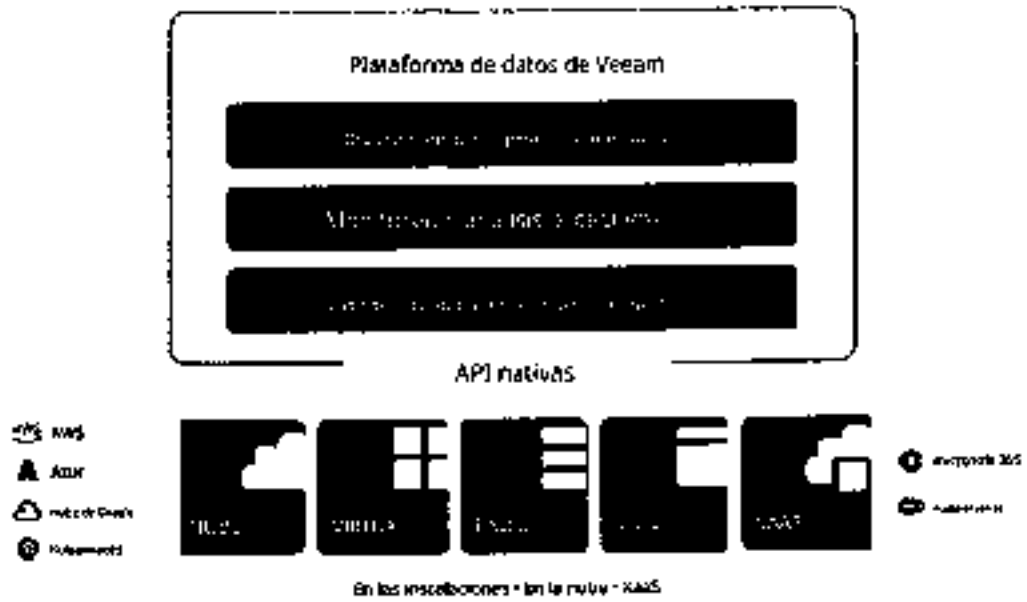
CONSORCIO EMDOC
EMDOC
Santo Domingo R.D.
06082023

© 2023 Software de Veeam. Información confidencial. Divulgación. Todos los derechos. Todos los demás productos son propiedad de sus respectivos dueños.

436

Producto

Cargas de trabajo protegidas



82
Promotor neto
Puntaje

450K+
clientes en todo el mundo están protegidos por Veeam

70%
de los Global 2000 son clientes de Veeam

81%
de Fortune 500 son clientes de Veeam

"Veeam proporciona una excelente protección de datos. Todos los que formaron parte del proceso de recuperación de ransomware están respirando aliviados".

—Kimberly La Grue,
CIO, ciudad de Nueva Orleans

CITY OF NEW ORLEANS

Leader 2023

Best Usability 2023

Most Likely to Recommend 2023

CONSORCIO EMDOC
EMDOC CONSORCIO
Santo Domingo, R.D.
08/08/2023

© 2023 Software de Veeam. Información confidencial. Propiedad intelectual protegida. Todas las marcas registradas son propiedad de sus respectivos dueños.

Traducido del inglés al español - www.onlinedoctranslator.com/es

VEEAM

VMCE

Veeam Backup & Replication v12: configurar, gestionar y recuperar

Duración: tres días

Teoría/laboratorios: 60/40

Descripción general

El veeamCopia de seguridad y replicación v12: El curso de capacitación Configurar, administrar y recuperar es un curso técnico de cinco días enfocado en enseñar a los profesionales de TI las habilidades para configurar, administrar y respaldar una solución Veeam Backup & Replication v12. Con amplios laboratorios prácticos, la clase permite a los administradores e ingenieros proteger y gestionar datos de forma eficaz en un entorno físico y empresarial en constante cambio, aportando beneficios tangibles a los empresas en el mundo digital.

Este curso se basa en Veeam Backup & Replication v12, parte de Veeam Data Platform.

Audiencia

Este curso es adecuado para cualquier persona responsable de configurar, gestionar o dar soporte a un entorno Veeam Backup & Replication v12.

Requisitos previos

Los asistentes deben tener experiencia fundamental en TI trabajando con redes, servidores, almacenamiento, nube, virtualización y sistemas operativos.

Para aprovechar al máximo este curso, los estudiantes deben estar familiarizados con los conceptos fundamentales básicos de Veeam Backup & Replication, ya sea a través de la experiencia práctica o mediante la capacitación en línea gratuita sobre Fundamentos de Veeam Backup & Replication.

Certificación

La finalización de este curso satisface el requisito previo para tomar el Veeam Certified Engineer (VMCE) examen v12.

Objetivos

Después de completar este curso, los asistentes deberían poder

- Describir los conceptos de seguridad de Veeam
- Diseñar una solución, configurar la infraestructura de respaldo y trabajos de copia de seguridad
- Enumerar los pasos de seguridad y configurar varias opciones de repositorio inmutable
- Describir las capacidades de replicación de Veeam
- Determinar el caso de uso apropiado para copias de seguridad, réplicas y protección continua de datos
- Configurar los componentes de la infraestructura de respaldo, incluidos servidores proxy y repositorios
- Dado un escenario, evaluar cuándo y cómo aplicar la configuración de inmutabilidad
- Describir escenarios, restaurar datos y copias de seguridad

CONSORCIO EMDOC
EMDOC
CONSORCIO
10083001
Santo Domingo, R.D.

© 2023 Veeam Software. Información confidencial. Todos los derechos reservados. Todas las demás marcas registradas son propiedad de sus respectivos dueños.

VMCE

Contenido

¿Qué se puede proteger?

- Revisión de Veeam Data Platform e introducción al escenario de clase.

Asegure su servidor de respaldo

- Describir estrategias y herramientas para proteger el servidor de respaldo de Veeam para evitar accesos no autorizados y fugas de datos

Coherencia de la aplicación con autenticación segura

- Logre copias de seguridad de máquinas virtuales consistentes con las aplicaciones mientras mantiene la autenticación segura del sistema operativo.

Proteger cargas de trabajo

- Proteja eficientemente las máquinas virtuales VMware y Hyper-V basándose en SLA bien definidos mediante la creación de trabajos de respaldo.

Agentes de protección de datos

- Identificar el uso de grupos de protección para automatizar la instalación de Veeam Agents y proteger cargas de trabajo con trabajos de respaldo de agentes.

Protegiendo NAS

- Enumere los componentes necesarios y las funciones disponibles para proteger las soluciones NAS

Optimización de la copia de seguridad

- Analizar características y configuraciones que permitan la optimización de almacenamiento de respaldo, respaldos más rápidos y consistencia de datos

Inmutabilidad

- Describir los mecanismos de protección de los datos de respaldo para evitar la eliminación prematura y modificaciones no deseadas.

Repositorio reforzado de Linux

- Identificar las características y los pasos de implementación de un repositorio reforzado de Linux para lograr la inmutabilidad de los datos de respaldo

Repositorio de almacenamiento de objetos

- Describir casos de uso, ventajas y consideraciones para implementar soluciones de almacenamiento de objetos como repositorio de respaldo de Veeam

Optimización de la infraestructura de respaldo

- Revisar las opciones de replicación y configuraciones disponibles para mejorar el rendimiento general de la solución de respaldo.

Replicación

- Describir casos de uso, arquitecturas y características de trabajos de replicación y políticas de protección continua de datos (CDP).

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.
14/08/2023

© 2023 VeeamSoftware. Información confidencial. Reservados todos los derechos. Todas las marcas registradas son propiedad de sus respectivos dueños.

VMCE

Verificación de copias de seguridad

- Garantizar la recuperabilidad y cumplir con la regla 3-2-1 con los trabajos de copia de seguridad.

Retención a largo plazo

- Emplear diferentes mecanismos para archivar datos, incluidas las políticas de retención de abuelo, padre e hijo.

Repositorio de respaldo escalable

- Diseñar la arquitectura, las políticas de ubicación, los niveles de datos y la gestión de repositorios de respaldo escalables (SOBR).

Mejor práctica de seguridad

- Identificar características para el endurecimiento de máquinas virtuales y copias de seguridad con VeeamZero.

Verificación de recuperación

- Crear pruebas automatizadas para garantizar la recuperabilidad en las copias de seguridad y réplicas.

Escenario empresarial de respaldo de Veeam

- Describir los casos de uso de Veeam Backup Enterprise Manager.

Escenario de recuperación: falla de la máquina virtual

- Elija entre diferentes métodos para recuperar una máquina virtual desde la copia de seguridad.

Escenario de recuperación: ataque de ransomware

- Recuperar forma segura un servidor después de un incidente de ransomware con instantáneas de volumen de hardware, desde la copia de seguridad y como parte del proceso de remediación.

Escenario de recuperación: recuperación de agente

- Explore las opciones disponibles para recuperar datos de máquinas de agentes de Windows.

Escenario de recuperación: recuperación de replicación

- Usar las capacidades de Veeam para recuperar elementos de máquinas virtuales desde copias de seguridad y réplicas.

Escenario de recuperación: recuperación de archivos individuales

- Restaurar archivos en sistemas operativos invitados y aplicaciones desde copias de seguridad a nivel de imagen y desde diversos dispositivos de almacenamiento.

Escenario de recuperación: recuperación desde la réplica

- Describir los equipos de la máquina virtual disponibles para recuperar una máquina virtual desde su réplica y los mecanismos para evitar la pérdida de datos y la recuperación de servicios interdependientes.

Escenario de recuperación: recuperación de NAS

- Explorar las opciones disponibles para recuperar archivos individuales desde copias de seguridad de archivos creadas desde la capa de seguridad.

Aprende más
www.veeam.com/vmce

Contáctenos
vmce@veeam.com

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.
10/05/2023

© 2023 Veeam Software. Información confidencial. Reservados todos los derechos. Todas las marcas registradas son propiedad de sus respectivos dueños.

Traducido del inglés al español - www.deepl.com/translator

vmware LEARNING

VMware vSphere: instalar, configurar, administrar

Resumen del curso

Este curso de cinco días presenta una capacitación práctica intensiva que se enfoca en la instalación, configuración y administración de VMware vSphere 8, que incluye VMware ESXi 8 y VMware vCenter 8. Este curso lo prepara para administrar una infraestructura de vSphere para una organización de cualquier tamaño.

Este curso es la base para la mayoría de las tecnologías de VMware en el centro de datos definido por software.

Objetivos del Curso

Al final del curso, usted debe ser capaz de cumplir con los siguientes objetivos:

- Instalar y configurar hosts ESXi
- Implementar y configurar vCenter
- Utilice vSphere Client para crear el inventario de vCenter y asignar funciones a los usuarios de vCenter
- Cree redes virtuales con conmutadores estándar y conmutadores distribuidos de vSphere
- Cree y configure almacenes de datos mediante tecnologías de almacenamiento compatibles con vSphere
- Usar vSphere Client para crear máquinas virtuales, plantillas, clones e instantáneas
- Cree bibliotecas de contenido para administrar plantillas e implementar máquinas virtuales
- Administre la migración de recursos de máquinas virtuales
- Migrar máquinas virtuales con VMware vSphere vMotion y VMware vSphere Almacenamiento vMotion
- Cree y configure un clúster de vSphere que esté habilitado con VMware vSphere Alta disponibilidad y VMware vSphere Programador de recursos distribuidos
- Administre el ciclo de vida de vSphere para mantener actualizados vCenter, hosts ESXi y máquinas virtuales

Público objetivo

- Administradores del sistema
- Ingenieros de sistemas

requisitos previos

Este curso tiene los siguientes requisitos previos:

- Experiencia en administración de sistemas en sistemas operativos Microsoft Windows o Linux

Certificación

Asistir a este curso cumple con el requisito de capacitación para lograr la siguiente certificación:

- Profesional certificado de VMware: Virtualización de centro de datos (VCP-DCV)

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD
HOJA DE DATOS

441

Opciones de entrega del curso

- Aula
- Vivo en línea
- Entrenamiento Privado

Alineación de productos

- VMware ESXi 8.0
- VMware vCenter 8.0

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo
HOJA DE DATOS

Módulos del curso:

1 Curso introductorio
- Presentaciones y logística del curso.
- Objetivos del Curso

2 Descripción general de vSphere y virtualización
- Explicar los conceptos básicos de virtualización
- Describir cómo encaja vSphere en el centro de datos definido por software y la infraestructura de la nube
- Reconocer las interfaces de usuario para acceder a vSphere
- Explicar cómo interactúa vSphere con las CPU, la memoria, las redes, el almacenamiento y las GPU.

3 Instalación y configuración de ESXi
- Instalar un host ESXi
- Reconocer las mejores prácticas de asignación de usuarios de ESXi
- Configure los ajustes del host ESXi mediante DCUI y VMware Host Client

4 Implementación y configuración de vCenter
- Reconocer la comunicación de hosts ESXi con vCenter
- Implementar el dispositivo de servidor vCenter
- Configurar los ajustes de vCenter
- Use vSphere Client para agregar y administrar claves de licencia
- Crear y organizar objetos de inventario de vCenter
- Reconocer las reglas para aplicar permisos de vCenter
- Ver registros y eventos de vCenter

5 Configuración de redes de vSphere
- Configurar y ver configuraciones de interruptores estándar
- Configurar y ver configuraciones de conmutadores distribuidos
- Reconocer la diferencia entre los conmutadores estándar y los conmutadores distribuidos
- Explicar cómo establecer políticas de red en conmutadores estándar y distribuidos

6 Configuración del almacenamiento de vSphere
- Reconocer las tecnologías de almacenamiento de vSphere
- Identificar tipos de almacenes de datos de vSphere
- Describir los componentes y el direccionamiento de Fiber Channel
- Describir los componentes y el direccionamiento de iSCSI
- Configurar almacenamiento local en ESXi
- Crear y administrar almacenes de datos VMFS
- Configurar y administrar almacenes de datos NFS

7 Implementación de máquinas virtuales
- Crear y aprovisionar máquinas virtuales
- Explicar la importancia de VMware Tools
- Identificar los archivos que componen una VM
- Reconocer los componentes de una VM
- Navegar por vSphere Client y examinar la configuración y las opciones de la máquina virtual
- Modificar las máquinas virtuales en ejecución y asignar nuevos recursos
- Cree plantillas de VM e implemente VM a partir de ellas
- Clone una VM
- Cree especificaciones de personalización para sistemas operativos invitados
- Cree bibliotecas de contenido locales, publicadas y suscritas
- Implementar una plantilla desde una biblioteca de contenido
- Administre múltiples versiones de plantillas de VM en bibliotecas de contenido

8 Administrar máquinas virtuales
- Reconocer los tipos de migraciones de máquinas virtuales que puede realizar dentro de una instancia de vCenter y entre instancias de vCenter
- Migrar máquinas virtuales con vSphere vMotion
- Describir la función de la compatibilidad mejorada de vMotion en las migraciones
- Migrar máquinas virtuales con vSphere Storage vMotion
- Realizar migraciones en caliente y en frío
- Administre, consolide y elimine instantáneas
- Describir los conceptos de CPU y memoria en relación con un entorno virtualizado
- Describa cómo las máquinas virtuales consumen los recursos
- Definir recursos compartidos de CPU y memoria, reservas y límites

9 Implementación y configuración de clústeres de vSphere
- Cree un clúster de vSphere habilitado para vSphere DRS y vSphere HA
- Ver información sobre un clúster de vSphere

vmware

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 EE. UU. Tel 877-486-9273 Fax 650-427-5001 www.vmware.com/es

Copyright © 2019 VMware, Inc. Todos los derechos reservados. Este producto está protegido por leyes y tratados internacionales y de propiedad intelectual. VMware considera que la información de este documento es precisa en la fecha de publicación inicial. La información está sujeta a cambios sin previo aviso. VMware no asume ninguna responsabilidad por errores que puedan aparecer en este documento. VMware no otorga ninguna garantía, expresa o implícita, en este documento. VMware, el logotipo de VMware y los productos de VMware mencionados en este documento son marcas comerciales o registradas de VMware, Inc. en los Estados Unidos y en otras jurisdicciones. Todas las demás marcas y nombres mencionados pueden ser marcas comerciales de sus respectivas empresas.

EXCEPTO LO EXPRESAMENTE ESTABLECIDO EN EL CONTRATO DE LICENCIA APLICABLE PARA UN PRODUCTO DE VMWARE, VMWARE NO ASUME NINGUNA RESPONSABILIDAD DE NINGÚN TIPO, INCLUYENDO LAS GARANTÍAS IMPLÍCITAS, CONDICIONES O DECLARACIONES RELATIVAS A SU PRODUCTO, INCLUIDA SU IDONEIDAD PARA UN FIN DETERMINADO, COMERCIABILIDAD O NO INFRACCIÓN. EN NINGÚN CASO VMWARE SERÁ RESPONSABLE DE LOS DAÑOS INDIRECTOS, ESPECIALES, INCIDENTALES O EMERGENTES (INCLUIDOS LOS DAÑOS POR PÉRDIDA DE BENEFICIOS, INTERRUPCIÓN DEL NEGOCIO O PÉRDIDA DE INFORMACIÓN) QUE SURJAN DEL USO O LA IMPOSIBILIDAD DE USO DE ESTE PRODUCTO, INCLUSO SI VMWARE HA SIDO EXPRESAMENTE ADVERTIDO DE LA POSIBILIDAD DE DICHOS DAÑOS. VMware no asume ninguna responsabilidad por la precisión o integridad de la información contenida en este documento. Los productos de VMware se proporcionan "TAL CUAL" y "SEGÚN DISPONIBILIDAD". VMware no asume ninguna responsabilidad por el resultado de la implementación, el uso o el rendimiento de los productos de VMware.

CONSORCIO EMDOC
EMDOC
SANTO DOMINGO, R.D.

- Explicar cómo vSphere DRS determina la ubicación de las máquinas virtuales en los hosts de clúster
- Reconocer casos de uso para la configuración de vSphere DRS
- Supervisar un clúster de vSphere DRS
- Describir cómo responde vSphere HA a varios tipos de fallas
- Identificar opciones para configurar la redundancia de red en un clúster de vSphere HA
- Reconocer las consideraciones de diseño de vSphere HA
- Reconocer los casos de uso para varias configuraciones de vSphere HA
- Configurar un clúster de vSphere HA
- Reconocer cuándo usar vSphere Fault Tolerance

10 Administrar el ciclo de vida de vSphere

- Habilite vSphere Lifecycle Manager en un clúster de vSphere
- Describir las funciones de vCenter Update Planner
- Ejecute comprobaciones previas de actualización en un vCenter e informes de interoperabilidad
- Reconocer las funciones de VMware vSphere Lifecycle Manager en el caso de uso dado
- Distinguir entre administrar hosts usando líneas base y administrar hosts usando imágenes
- Describir cómo actualizar hosts utilizando líneas de base
- Describir imágenes de ESXi
- Valide el cumplimiento del host ESXi con una imagen de clúster y actualice los hosts ESXi
- Actualizar hosts ESXi mediante vSphere Lifecycle Manager
- Describir las recomendaciones automáticas de vSphere Lifecycle Manager
- Use vSphere Lifecycle Manager para actualizar VMware Tools y el hardware de VM

Contáctenos

Si tiene preguntas o necesita ayuda para registrarse en este curso, haga clic en azul.

vmware

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

Copyright © 2021 VMware, Inc. Todos los derechos reservados. Este producto está protegido por leyes de derechos de autor y propiedad intelectual de EE. UU. e internacionales. VMware considera que la información de este documento es precisa en la fecha de publicación inicial. La información está sujeta a cambios sin previo aviso. VMware no asume ninguna responsabilidad por errores que puedan aparecer en este documento. VMware no otorga ninguna garantía, expresa o implícita, en este documento. El usuario es responsable del cumplimiento de todas las leyes de derechos de autor aplicables. Sin limitar los derechos de autor, ninguna parte de este documento puede ser reproducida, almacenada o introducida en un sistema de recuperación, ni transmitida de ninguna forma o por ningún medio (electrónico, mecánico, fotocopia, grabación o de otro tipo) para ningún propósito, sin el permiso expreso por escrito de VMware. Es posible que VMware tenga patentes, solicitudes de patentes, marcas comerciales, derechos de autor u otros derechos de propiedad intelectual sobre el contenido de este documento. Excepto que se proporcione expresamente en un contrato de licencia por escrito de VMware, el suministro de este documento no le otorga ninguna licencia a estas patentes, marcas comerciales, derechos de autor u otros derechos de propiedad intelectual.

VMware se reserva el derecho de interpretación y modificación de este aviso de derechos de autor y la política de uso de derechos de autor de VMware en general.

VMware y el logotipo de VMware son marcas comerciales o marcas comerciales registradas de VMware, Inc. en los Estados Unidos y en otras jurisdicciones. Todas las demás marcas y nombres mencionados en este documento pueden ser marcas comerciales de sus respectivos propietarios.

VMware, Inc. en los Estados Unidos y en otras jurisdicciones.

CONSORCIO EMDOC
EMDOC
RUC 20600...

Traducción del inglés al español - www.onlinedoctranslator.com/es/

BROADCOM

VMware vSphere Estándar

Documentación específica del programa ("SPD")

El(los) programa(s) de software de Broadcom ("Software de Broadcom") que se enumera(n) a continuación se proporciona conforme a los siguientes términos y condiciones, además de los términos y condiciones a los que se hace referencia en la cotización, el formulario de pedido, la declaración de trabajo o cualquier documento de pedido equivalente mutuamente de Broadcom (cada uno de ellos, un "Documento de transacción") conforme al acuerdo de suscripción final o contrato de licencia (en conjunto, el "Acuerdo") celebrado entre el Cliente y la empresa de Broadcom ("Broadcom") a través de la cual el Cliente obtuvo una licencia para el Software de Broadcom. Estos términos entrarán en vigor a partir de la fecha de vigencia de dicho Documento de transacción. Los términos en mayúsculas tienen los significados que se les atribuyen en el presente documento o, de otro modo, en el Acuerdo.

Nombre del programa. *VMware vSphere Estándar*

1. DEFINICIONES.

Todos los términos definidos en el Glosario de software de Broadcom ubicado en https://www.broadcom.com se aplican a esta SPD a menos que se especifique aquí.

"BIOS" significa Sistema básico de entrada y salida, un conjunto de rutinas que inicia el sistema operativo y configura el hardware del procesador.

"Servicios en la nube" significa servicios de infraestructura informática y de plataforma (como recursos informáticos, capacidades de almacenamiento, bases de datos o máquinas virtuales y otros servicios de infraestructura informática y de plataforma) que un tercero pone a disposición de los clientes para su consumo.

"Centro" significa una única unidad computacional física del Procesador.

"Instancia" significa una única instalación del Software en un servidor físico o una máquina virtual.

"Aplicación desarrollada internamente" significa (i) una aplicación informática que el Cliente ha creado o desarrollado y (ii) una o más aplicaciones informáticas de terceros que son accesibles al servicio basado en aplicaciones del Cliente, y (b) no pueden ser accedidas directamente por los usuarios finales del servicio basado en aplicaciones del Cliente.

"Procesador" significa un único chip físico que alberga al menos un núcleo que puede ejecutar programas de computadora.

"Servidor" significa un sistema de hardware capaz de ejecutar el software del servidor. Una partición o blade de hardware se considera un sistema de hardware independiente.

2. DERECHOS DE USO Y LIMITACIONES.

Métricas de licencia

- VMware vSphere Standard ("VVS") es un software de suscripción con licencia por núcleo con un requisito de licencia mínima de 16 núcleos por procesador.
- Cada núcleo del servidor debe tener licencia, incluidos los núcleos desactivados por el BIOS. La cantidad de licencias de núcleo requeridas es igual a la cantidad de núcleos del servidor, sujeta al mínimo de 16 licencias de núcleo por procesador.

CONSORCIO EMDOC
EMDOC
Santo Domingo, R.D.

- El Cliente puede utilizar el Software VVS en un Servidor que contenga hasta la cantidad máxima de núcleos por los cuales el Cliente haya pagado las tarifas de licencia correspondientes.

Derechos de uso y Limitaciones

- **Servidor vCenter.** vCenter Server se puede utilizar para proporcionar capacidades de administración centralizada a cualquier entorno de infraestructura VMware by Broadcom con licencia y con una suscripción activa a Servicios de soporte y suscripción.
- **Restricciones de uso con servicios de nube pública.** El Cliente no debe y no debe permitir que los Agentes Externos del Cliente: usar o implementar el Software en ningún Servicio en la Nube.
- **Derechos y restricciones de alojamiento.** El Cliente puede utilizar el Software para entregar Aplicaciones desarrolladas exclusivamente como un servicio a un tercero a través de una red interna o externa, Salvo que se indique expresamente en este párrafo y en el Contrato de licencia, el uso del Software o para cualquier otro tipo de alojamiento o para el beneficio de un tercero de cualquier manera está estrictamente prohibido a menos que el Cliente sea un participante autorizado en un programa de VMware que se rija por un conjunto independiente de términos y condiciones que autorice dicha Actividad.

3. INFORMACIÓN Y TÉRMINOS DE TERCEROS.

Todos los términos de licencia de software de terceros requeridos se incorporan a esta referencia y se establecen en la documentación en línea en techdocs.broadcom.com o legal.broadcom.com.

- **Herramientas de VMware.** VMware Tools es un conjunto de utilidades y controladores que se pueden instalar en un sistema operativo invitado para mejorar el rendimiento y la funcionalidad de un sistema operativo invitado cuando se ejecuta en una máquina virtual junto con un hipervisor vSphere. El cliente no puede utilizar VMware Tools con ningún otro hipervisor. El cliente puede distribuir VMware Tools a terceros únicamente cuando se instala en un sistema operativo invitado dentro de una máquina virtual. El cliente es responsable del cumplimiento por parte de dichos terceros de los términos y condiciones del Acuerdo marco.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

Productos Nuevos
Productos
Aplicaciones Móviles
Suministros y Accesorios
Soporte y Controladores
Dónde Comprar
Noticias
Recursos y Aprendizaje
Contáctenos

IMPRIMIR ESTA PÁGINA ENVIAR ESTA PÁGINA

CanoScan LIDE 300

Escáneres para Fotografías

Dónde Comprar



CONSORCIO EMDOC
EMDOC
Santo Domingo, R.D.

Información General | Características | Especificaciones
Contenido de la Caja | Servicio y Soporte | Folletos y Manuales
Controladores y Software | Preguntas Frecuentes

Información General

ESCANEO SENCILLO Y COMPACTO
El escáner CanoScan LiDE 300 facilita el escaneo de documentos y fotografías. Con el escaneo rápido de 10 segundos[1], 4 botones "EZ" y una resolución de 2400 x 2400 ppp[2], el escáner CanoScan LiDE 300 ofrece características superiores en un tamaño compacto.



1. La velocidad de escaneo de un documento en color (Carta/A4 en color, 300 ppp) se mide con ISO/IEC 29183 Target-A. La velocidad de escaneo de una fotografía en color (Color, 4" x 6", 300 ppp) se mide con ISO/JIS-SCID núm. 2. La velocidad de escaneo indica el tiempo transcurrido desde que se presiona el botón de escaneo de software controlador del escáner hasta la desactivación de la pantalla de despliegue de estado. La velocidad de escaneo se mide mediante una interfaz USB 3.0 en una PC con el cable USB incluido y puede variar de acuerdo con la configuración del sistema, la interfaz, el software, las configuraciones del modo de escaneo y el tamaño del documento, entre otros.
2. La resolución óptica es una medida de la resolución máxima de muestreo del hardware con base en la norma ISO 14473. El aumento de la resolución de escaneo incluye la posible área máxima de escaneo.
3. El Modo de Escaneo Automático está disponible al escanear desde una computadora mediante el software IJ Scan Utility o IJ Scan Utility Lite y al seleccionar la característica de 1 clic y luego "Guardar en la PC", o usando el botón del modo de escaneo automático "EZ" en modelos seleccionados. El Modo de Escaneo Automático no está disponible en el modo de escaneo vertical.
4. La extracción de textos de imágenes escaneadas (OCR [Reconocimiento óptico de caracteres]) sólo está disponible cuando se extrae texto al escanear con las configuraciones para documentos, personalizadas o del software controlador mediante el software IJ Scan Utility/IJ Scan Utility Lite en un sistema operativo compatible. Para mayor información, referirse al Manual de Usuario del producto.
5. Requiere una conexión de Internet. Requiere una cuenta de servicio activa en la nube y el software requerido debe instalarse en la computadora para que la función "Enviar a la Nube" funcione con estos servicios.
6. Se requiere la Plataforma .NET Framework 4 para la instalación con el sistema operativo Windows®. Los formatos compatibles de fotografías son PDF (sólo las creadas mediante el PDF Creator de Canon), JPEG (Exif), TIFF y PNG. Los formatos de video compatibles son MOV (solamente de ciertas cámaras digitales Canon) y MP4 (solamente de ciertas videocámaras digitales Canon).
7. Solo puede garantizar la operación en una PC con Windows 10, Windows 8.1 o Windows 7 SP1 previamente instalados.
8. Se requiere una conexión a Internet durante la instalación del software. Para lograr una compatibilidad completa con macOS, se requiere de la v10.13 o posteriores.
9. El escáner controlador del escáner "ScanGear MP para Linux" debe estar instalado cuando se escanea en el sistema operativo Linux. Pueden aplicar ciertas excepciones.

Canon U.S.A., Inc.

447-A

Canon CanoScan LiDE 300(2995C010)
Canon CanoScan LiDE 300 - Flatbed scanner - A4/Letter - 2400 dpi x 2400 dpi - USB 2.0



Compact and affordable,this lightweight scanner is perfect for those wanting straightforward scanning at the touch of a button.

Key Selling Points

Compact,sleek and affordable scanner for home or office
Pristine borderless prints
Instant access
Freedom of the cloud
Maximize your money
Get creative

Product Features

Compact,sleek and affordable scanner for home or office

With a sleek,compact and stylish design,this lightweight A4 flatbed scanner is fitted with 4 EZ operation buttons for easy use and hassle free scanning. Perfect for high-resolution scanning at home or in the office.

Pristine borderless prints

Effortlessly print stunning borderless photos from 4x6 inch to A4,filled with fine detail and documents with sharp text for high-quality results

Instant access

Enjoy straightforward printing,copying and scanning using your smartphone or tablet or directly access cloud storage via PIXMA Cloud Link - all thanks to the Canon PRINT app

Freedom of the cloud

Print and scan documents to cloud services such as GoogleDrive,OneDrive and Dropbox. You can also attach and send scanned files directly via email - all without a PC.

Maximize your money

Cut waste and boost your cost savings by up to 50% compared to standard cartridges with optional XL ink cartridges and auto 2 sided printing.

Get creative

Unleash your inner artist with Creative Park and the Easy PhotoPrint Editor. Use the app to design cards,calendars and more using photos from your tablet,PC or cloud.

Main Specifications

Product Description	Canon CanoScan LiDE 300 - flatbed scanner - desktop - USB 2.0
Device Type	Flatbed scanner - desktop
Interface Type	USB 2.0
Scan Element Type	Contact Image Sensor (CIS)
Light Source	3 colour RGB LED
Additional Functions	Scan to cloud
Max Supported Document Size	216 x 297 mm
Input Type	Colour
Grayscale / Color Depth	16-bit (64K grey levels) / 48-bit colour
Grayscale / Color Depth (External)	8-bit (256 grey levels) / 48-bit colour
Optical Resolution	2400 dpi x 2400 dpi
Interpolated Resolution	19200 dpi
Max Document Size	216 mm x 297 mm

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

447-B

Supported Document Type	Plain paper,bulk objects (such as books,magazines and other bound materials)
System Requirements	Microsoft Windows 7,Microsoft Windows 7 SP1,Windows 8.1,Windows 10,Apple MacOS X 10.12 - 10.13,Apple MacOS X 10.11.6
Dimensions (WxDxH)	25 cm x 36.7 cm x 4.2 cm
Weight	1.7 kg

Extended Specification

General

Type	Flatbed scanner - desktop
Interface Type	USB 2.0
Additional Functions	Scan to cloud
Max Supported Document Size	216 x 297 mm

Scanner

Input Type	Colour
Grayscale Depth	16-bit (64K grey levels)
Grayscale Depth (External)	8-bit (256 grey levels)
Colour Depth	48-bit colour
Colour Depth (External)	48-bit colour
Optical Resolution	2400 dpi x 2400 dpi
Interpolated Resolution	19200 dpi
Scan Element Type	Contact Image Sensor (CIS)
Bulb / Light Source Type	3-colour RGB LED
Control Panel Buttons Functions	Copy,AutoScan,send to,PDF
Scanner Speed Details	10 sec/scan - colour - A4 - 300 dpi 5 sec/scan - colour - 4x6 - 300 dpi 9 sec/scan - preview 14.8 ms/line - colour - 2400 dpi 6.6 ms/line - colour - 1200 dpi 3.8 ms/line - colour - 600 dpi 2.2 ms/line - colour - 300 dpi 4.3 ms/line - greyscale - 2400 dpi 2.2 ms/line - greyscale - 1200 dpi 1.3 ms/line - greyscale - 600 dpi 2.2 ms/line - greyscale - 300 dpi
Scanner Features	Auto Document Fix,Auto Scan Mode,Auto Photo Fix,4 EZ Buttons,Advanced Z-lid Expansion Top

Media Handling

Max Document Size	216 mm x 297 mm
Supported Document Type	Plain paper,bulk objects (such as books,magazines and other bound materials)

Expansion / Connectivity

Interfaces	USB 2.0 - Mini-B

Miscellaneous

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo RD

447-C

Cables Included	1 x USB cable

Power

Power Consumption Operational (Standby)	4.5 Watt
Power Consumption Stand by	0.3 Watt

Software / System Requirements

Software Included	Drivers & Utilities
OS Required	Microsoft Windows 7,Microsoft Windows 7 SP1,Windows 8.1,Windows 10,Apple MacOS X 10.12 - 10.13,Apple MacOS X 10.11.6

Dimensions &Weight

Width	25 cm
Depth	36.7 cm
Height	4.2 cm
Weight	1.7 kg

Environmental Parameters

Min Operating Temperature	5 °C
Max Operating Temperature	35 °C
Humidity Range Operating	10 - 90% (non-condensing)

What's in the box

Canon CanoScan LiDE 300
USB cable
Drivers &Utilities

Product data is provided by CNET,we do not warrant the accuracy and completeness of the material contained in this data sheet

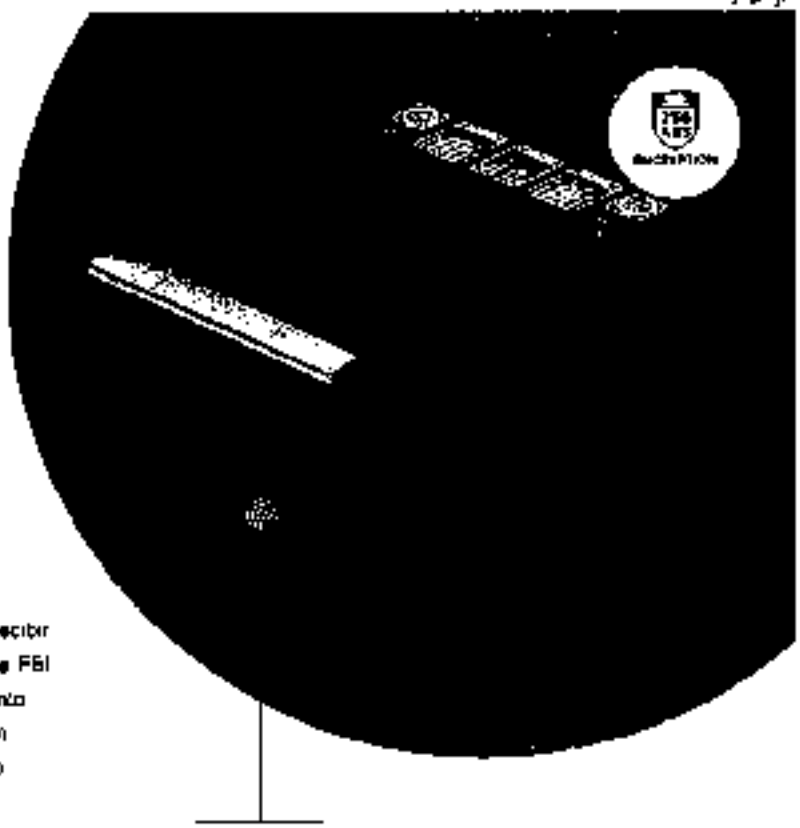
CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo RD

INTEGRATED BIOMETRICS

Kojak

Robusto, compacto, certificado por el FBI escáner FAP 60 de 10 impresiones

- Rechazo automático de dedo falso
- Detección automática basada en software



El Kojak acaba con el mito de que los escáneres de huellas dactilares 4-4-2 FAP 60 deben ser grandes, pesados y deben recibir mucha energía. Esta unidad compacta y ligera, certificada por el FBI según las especificaciones del Apéndice F, ofrece un rendimiento rápido para la inscripción y verificación de 10 impresiones en un formato compacto que utiliza menos energía que cualquier otro escáner FAP 60 disponible actualmente.

Kojak viene con una interfaz gráfica intuitiva basada en LED que hace que el registro preciso de escaneo sea rápido y fácil. Una versión con etiqueta de su propia marca incluye personalización para OEM y proveedores de soluciones de gestión de identidad.

Disponible en versiones integradas e autónomas.

- Comunicaciones cifradas entre el escáner y la aplicación host
- Permite el registro y la verificación rápidos con 10 dedos, certificado por el FBI según las especificaciones del Apéndice F
- Interfaz gráfica de usuario LED
- Diseñado para aplicaciones más grandes
- El consumo de energía más bajo de cualquier escáner FAP 60 compatible
- Etiquetado privado opcional

Características Y Beneficios

Rápido

- Captura rápida de dedos secos
- No es necesario limpiar impresiones latentes en situaciones de gran volumen
- Fácil integración a través de un solo SDK para todos Productos biométricos integrados certificados por el FBI

Mejor

- No se ve afectado por temperaturas extremas, luz solar directa o luces artificiales brillantes
- Compacto, ligero y resistente
- Rechaza los ataques comunes de suplantación de posición
- No emite luces brillantes durante los escaneos
- Cumple o supera las especificaciones de durabilidad militar de EE. UU.

Inteligente

- Precios competitivos
- Consumo de energía extremadamente bajo
- Elimina consumibles (membranas de silicona o cinta de limpieza)
- Menores costes de mantenimiento

El Kojak encripta comunicaciones entre el scanner y aparatos externos o aplicaciones usando claves 256-bit AES y algoritmos RSA. Este técnico de circuito cerrado protege la data biométrica al momento de adquisición, a través de un cableado, y en la aplicación servidora. Combinando los microchips de seguridad ya integrados, las estructuras privadas/públicas de claves, y las mejores prácticas de la industria, el Kojak asegura que la información personal delicada reciba codificación del nivel más alto disponible actualmente para los scanners.

El Kojak también contiene protección contra la suplantación a través de un archivo único de calibración que está instalado durante la producción de cada aparato sensorizado. Cuando alguien intenta superar el sistema de seguridad del Kojak por desbloqueo, ataque o daño al hardware, se altera la calibración del aparato y las imágenes se quedan inservibles.

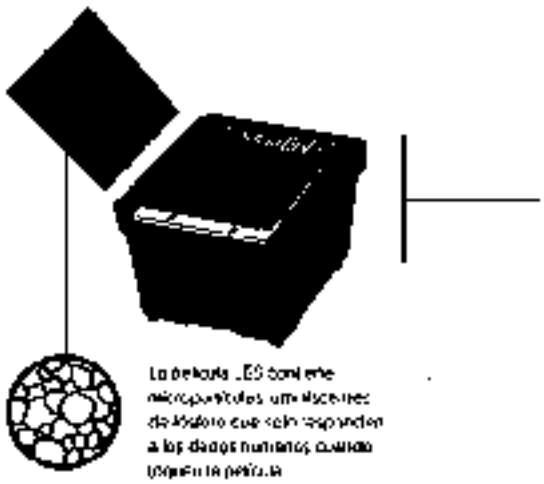
Para obtener más información sobre Kojak, visítenos en integratedbiometrics.com/products/kojak

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

La Tecnología Emisora De Luz

Los scanners de Integrated Biometrics usan nuestra tecnología emisora de luz patentada (LES) para producir imágenes de huella digital fijas, móviles, y certificadas por el FBI. Para hacer ese, utilizamos un scanner excepcionalmente durable y ágora.

Para obtener más información, vaya a integratedbiometrics.com/technology



La película LES contiene microcapacitores simétricos de silicio que son sensibles a los datos humanos cuando toca la película

Resistencia automática a la suplantación

La película LES de Integrated Biometrics puede distinguir entre las huellas digitales falsificadas y las reales. Los scanners LES rechazan automáticamente las huellas digitales que se produzcan con silicona, pegamento, goma, u otros materiales comunes para la suplantación.

Software auto-detector

Kojak automáticamente elige la captura de huella digital que genere la imagen de alta calidad sin intervención del suario. Los desarrolladores de aplicaciones pueden activar esta característica a través del kit de software desarrollador producido por Integrated Biometrics.

IB Scan Ultimate Capture SDK

Todo o Kojak é fornecido com o Software SDK de Captura Ultimate da IB. O SDK contém funções de API completas, necessárias para tarefas de registro de 10 impressões. Entre as funções de API suportadas estão:

- Captura automática dinâmica de cuatro dedos planos simultáneamente.
- Segmentación de cuatro dedos.
- Captura de impresión de desplazamiento fácil con detección de manchas
- Clasificación NFIQ individual por imágenes planas segmentadas e imágenes de desplazamiento individuales
- Verificación de secuencia para detección de dedo o mano incorrecta
- Captura superior de dedos dañados o secos sin requerir una almohadilla de silicona a través de nuestra tecnología "Toque en la película" ("Touch On Film")
- Las imágenes capturadas se pueden entregar a la aplicación en los formatos WSK, RAW, BMP, JPEG2000 y PNG

VERSIONES DISPONIBLES	NÚMERO DE PIEZA	DESCRIPCIÓN
Kojak 3.0 scanner de diez impresiones planas - DT	KJ210D4-E00	USB A 183/72
Kojak 3.0 scanner de diez impresiones planas - Module	KJ210SM-E00	Molex 8/9
Kojak 3.0 scanner de diez impresiones planas - AIC Kit DT	KJAICKT-001	USB A 183/72
Kojak 3.0 scanner de diez impresiones planas - AIC Kit Module	KJ210D4-E00	USB A 183/72

ACERCA DE INTEGRATED BIOMETRICS

Integrated Biometrics (IB), pionera en tecnología biométrica, diseña y fabrica un avanzado software SDK de identificación sin contacto de alta resolución y los sensores de huellas dactilares más móviles, curaderos y confiables del mundo, certificados por el FBI. Organizaciones policiales, militares, de seguridad nacional, de identidad nacional, de validación de elecciones, financieras y de servicios sociales de todo el mundo confían en los productos de Integrated Biometrics para llevar un registro, una identificación y una verificación rápidos y precisos, incluso en lugares remotos y en condiciones extremas.



integratedbiometrics.com
+1 888 845-8034
sales@integratedbiometrics.com

EMDOC CONSORCIO Santo Domingo, R.D.

ESPECIFICACIONES KOJAK/KOJAK PL

Soporte OS & Requisitos de Sistema

Soporte OS
- Ediciones Windows Desktop 7, 8, 10, 11
- Linux Kernel 4.0 o más reciente (32/64 bit, ARMv6, ARMv7)
  - Ubuntu 18.04, 20.04 o más reciente
  - Debian 10, 11, o más reciente
- Android 10, 11, 12

CPU
- x86 y x64 | 2.0GHz o superior ARM | 1.0 GHz o superior

Memoria
- 512MB o superior

Imágenes & Captura

Tipo de Sensor
- LES

Cámara
- CMOS

Resolución
- 500 ppi

Escala de Grises
- 256 rango dinámico en escala de grises

Tamaño de Imagen
- 1600 x 1500 pixels

Formatos de Imagen Admitidos
- RAW, JPEG2000, BMP, PNG, WSQ (FBI-aprobado)

Funciones: Botones Táctiles
- 2x botones táctiles programables*

Notificaciones: Auditivas y Visuales
- Timbre programable incorporado
- 10x LEDS rojos/verdes programables*

Cifrado
- 256-bit AES keys y RSA algoritmos

Certificaciones de Imagen/FBI
- FBI Appendix F, FAP 60

Velocidad
- Tasa de cuadro mínimo > 6 fps

Interface API
- Captura con un dedo o con varios dedos; Captura de huellas dactilares rodadas; Soporte multidispositivo/multiprocesador

Puntuación de Calidad
- NFIQ v1 soportado en todos los OSes y NFIQ2 para Windows

Peso & Dimensiones

Peso del Producto
- 725 gramos / 1.6 lbs

Tamaño del Platen
- 88,9 mm x 80,0 mm / 3.5" x 3.1"

Área de Detección
- 81.2 mm x 76.3 mm / 3.2" x 3.0"

Dimensiones del Ensamblaje del Escáner
- 114.7 mm x 131.9 mm x 82mm / 4.5" x 5.1" x 3.2"

Alimentación y Conectores

Interface
- USB 2.0

Fuente de Alimentación
- USB Host

USB Nivel de Voltaje USB
- 4.40V a 5.25V; 4.4via USB: escaneo completo > 300mA, tipico > 250mA

Conformidad & Certificaciones

Certificaciones USB
- USB-IF USB.ORG

Conformidad FCC/CE
- FCC Parte 15 (por ANSI C63.4: 2014) Clase B. CSA ICES-003 Clase B. CE Emisiones: EN 55022:2010 Class B. CE Immunity EN 55024:2010/A1:2015/A2:2020, IEC 61000-4-2

Descarga de Aire/Descarga de Contacto
- En conformidad con IEC 61000-4-2

Seguridad del Equipo
- IEC 62368-1

Material Peligroso
- RoHS Directive 2002/95/EC, TSCA, Proposición 65, Prohibición Canadá

Test de Vibración
- IEC 60068-2-64

Certificaciones
- Formatos de salida de plantillas de huellas dactilares
  - ISO_19794_2_2005/2011, ISO_19794_4_2005/2011
  - ANSI_INCITS_378_2004/ANSI_INCITS_381_2004
- 500 PPI rollos y planos de soporte de captura de huellas dactilares
- ISO 9001:2015
- Ibeta ISO 30107-3 en conformidad
- MOSIP en conformidad

Temperatura & Humedad

Temperatura Operativa
- -10°C ~ +55°C / 14°F ~ 131°F

Humedad
- 20~95% RH < 40°C / 104°F (sin condensación)

Temperatura de Almacenamiento
- -30°C ~ +60°C / -22°F ~ 140°F

Superficie & Sistemas

Protección de Ingreso/Agua/Polvo
- IP65 Diseñado a la superficie de escaneo

Durabilidad de la Superficie
- MIL-C-675c 4.5010, MIL-STD-810F

Limpieza y Desinfección
- Para limpieza y desinfección adecuadas de los productos IB, visite integratedbiometrics.com/cleaning

Tiempo Medio Entre Fallos (MTBF)
- Basado en 200 rollos diarios completos de 10 dedos, el MTBF de Kojak es de 22.2 años.



*No aplicable a las variantes de Kojak PL

451



Modelo T-LBK750

Dispositivo LCD para captura electrónica de firmas, con pantalla interactiva

El modelo SigLite LCD 4x3 de Topaz Systems, Inc. es un versátil sistema electrónico para la captura electrónica de firmas con pantalla electrónica integrada. La pantalla LCD muestra la 'tinta electrónica' bajo la punta del bolígrafo a medida que el usuario va escribiendo, permitiéndole así firmar de manera sencilla y natural. La pantalla también permite el texto y gráficos interactivos, y la pulsación de bolígrafo en los puntos activos, lo que permite a los usuarios leer los contratos y navegar por las pantallas de datos antes de firmar. El modelo SigLite LCD 4x3 ofrece la ventaja adicional de incorporar las poderosas herramientas de software y asistencia técnica de Topaz, incluyendo herramientas de desarrollo ActiveX, Java y J2ME, C++, y .NET, además de complementos de MS Office y Adobe Acrobat para la captura, codificación, formato y procesamiento seguro de firmas.

Tipo de sensor	Tablero táctil
Tipo de bolígrafo	Pluma plástica
Dimensiones	7.1" x 6.3" x 2.0" 180 x 160 x 52mm
Área de firma	4.4" x 2.5" 112 x 64mm
Resolución de pantalla	240x128
Tasa de conversión de datos	377 puntos por segundo
Resolución de captura	410 puntos reales por pulgada
Asistencia técnica	Se ofrecen actualizaciones sin costo
Capacidad de autenticación	Calidad forense de datos .SIG con capacidad de examen y autenticación con software SigAnalyze™ de Topaz (patente estadounidense 6,307,955)
Garantía	1 año, con opción de renovación

Software incorporado

Herramientas para programadores
ActiveX
Java y J2ME
C++
.NET
Tablet PC
Unix/Linux

Complementos
MS Word, Excel, Adobe Acrobat

Aplicaciones y utilidades
SigPlus Adjust
SigTool Imager
SignMeIn

Verificación
SigValid
SigCompare
SigAnalyze



www.topazsystems.com
650 Cochran Street Suite 6 Simi Valley, CA 93065, EE.UU.
Teléfono: (805) 520 – 8282 Fax: (805) 520 – 0867

TOPAZ SYSTEMS INC.

2006 - 2009 Topaz Systems, Inc.

Especificaciones sujetas a cambios sin previo aviso

EPSON
EXCEED YOUR VISION

Impresora térmica TM-T20III

Punto de venta



La solución económica, eficiente e ideal para el comercio de las pequeñas y medianas empresas

Características principales

- **Solución de impresión accesible:** destaca con la usabilidad y flexibilidad que el retail necesita.
- **mPOS/soporte para tabletas:** soporta Ethernet incluyendo Epson ePOS SDK (iOS/Android).
- **Mayor velocidad:** velocidad de impresión de hasta 250 mm/s.
- **Impresión flexible:** imprime desde móvil con Epson ePOS™.
- **Servicio y soporte*:** equipo de soporte técnico dedicado y soluciones personalizadas; garantía limitada de 3 años.

La impresora térmica TM-T20III imprime textos y gráficos en recibos a velocidades de hasta 250 mm/s, así como voptapos, cupones y códigos de barras de forma nítida.

Aprovecha las características que facilitan su uso, como la carga rápida de papel, el cortador automático y los indicadores LED. Con las opciones para reducir el consumo de papel en un 30%, y un promedio de duración antes de la falla de 360,000 horas, tendrás la excelente confiabilidad que esperas de una impresora Epson.

Thermal Line

3
Garantía de tres años

CONSORCIO EMDOC
EMDOC
Santo Domingo, R.D.

453

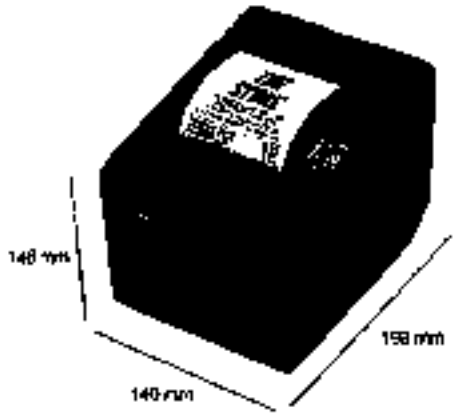
Epson TM-T20III

Especificaciones técnicas

EPSON
EXCEED YOUR VISION

Método de impresión	
	Impresión térmica de línea
Velocidad de impresión	
	250 mm/s (9,84 pulg/s)
Fuentes	
	9 x 17 y 12 x 24 caracteres (ancho x alto)
Capacidad de caracteres	
Estándar:	Papel de 80 mm de ancho: 48/64 Papel de 58 mm de ancho: 35/46
Modo de 42 columnas:	Papel de 80 mm de ancho: 42/50 Papel de 58 mm de ancho: 42/51
Tamaño de caracteres	
	0,85 mm x 2,13 mm y 1,25 x 3 mm (ancho x altura)
Juego de caracteres	
	95 alfanumérico, 16 set internacional, 128 x 40 gráfico
Código de barras	
	UPC-A, UPC-E, JAN13 (EAN13), JAN8 (EAN8), CODE39/32/128 ITF, CODABAR (NW-7), GS1-128, GS1 DataBar, Código bidimensional: PDF417, QRCode, MaxiCode, 2D GS1 DataBar, Simbología compuesta, Datamatrix, Aztec
Caracteres por pulgada	
	22,6 y 16,9
Dimensiones del papel	
	80 mm diámetro de rollo a 0,5 mm (3,15" a 0,02" x 3,27") 58 mm diámetro de 57,5 ± 0,5 mm a 83 mm (2,26" ± 0,02" x 3,27")
Confiabilidad	
	Tiempo medio antes de fallas: 360.000 horas Ciclo medio antes de fallas: 60.000.000 líneas Cortador automático: 1,5 millones de cortes
Interfaz	
	USB + serial o USB + Ethernet
Fuente de alimentación	
	100 VCA – 240 VCA, 50 Hz - 60 Hz
Consumo de energía	
	Modo operación: 29,5 W Modo en reposo: 2,8 W
Fuente de poder	
	Externa (Cable AC incluido)
Función D.I.C.O.	
	Sí (2 drivers)

Dimensiones (Ancho x Prof. x Altura)	
	5,51" x 7,83" x 5,75" (ancho x prof. x altura) 14 cm x 19,9 cm x 14,6 cm
Peso	
	3,75 lb / 1,7 kg
Color	
	Ebony/Negro
Accesorios estándar	
	Rollo de papel (1 rollo para probar el movimiento inicial de la impresora), CD-ROM, tapa del interruptor de encendido, cinta impermeable del interruptor de encendido, soporte para colgar la impresora de la pared, tornillos para colgar la impresora de la pared, patas de goma para la instalación vertical, panel de encaje de papel para instalación vertical, placa para orientación de papel de 58 mm de ancho, cable de interfaz (solo USB), cable de CA
Opciones de fijación	
	Cinta adhesiva y unidad de montaje externa
Normas de seguridad	
	UL 60950-1/CSA C22.2 N.° 60950-1
Controladores	
Sistemas operativos	Software instalador y controladores JavaPOS™, OPOS™, JavaPOS™, OPOS .NET™, controlador de puerto TM Virtual, controlador Linux® Cups, controlador Mac OS® X, Utilidad TM-T20III, EpsonNet Simple Viewer (Windows®, Mac®), ePOS-SDK
Imprimir desde móvil	Sistemas operativos implementados (iOS, Android™ y Windows®)
Epson ePOS	Servicio ePOS para impresión directa desde dispositivos móviles o aplicaciones de red
Instalación	
	Horizontal / vertical en mostrador / vertical en la pared con soporte
Garantía	
	Garantía limitada de 3 años
Contenido de la caja	
	TM-T20III Papel térmico en rollo (rollo inicial para control del funcionamiento) Cable de CA (dependiendo del modelo) Soporte para colgar la impresora de la pared Guía de configuración



Better Products for a Better Future

Para mayor información acerca de programas ecológicos de Epson, visite: eco.epson.com

En Latinoamérica, contactar a la oficina local o a tu distribuidor autorizado. Sucursales de Epson:

Epson Argentina, S.R.L. (5411) 5167 3000	Epson Chile, S.A. (562) 24843400	Epson Colombia, Ltda. (571) 523 3000	Epson Centroamérica (506) 2586 7800	Epson México, S.A. de C.V. (5255) 1323 2000	Epson Perú, S.A. (511) 418 0210	Epson Venezuela, S.R.L. (5802) 905 11 11 RIF: J-00138006-0	Epson Ecuador 1-800-000344

CONSORCIO EMDOC
EMDOC.com

Las especificaciones de Epson están sujetas a cambio sin previo aviso. Epson, EXCEED YOUR VISION y sus logotipos son marcas comerciales de Seiko Epson Corporation. Los demás nombres de productos y marcas son propiedad de sus respectivos dueños. Epson renuncia a cualquier derecho sobre estas marcas. © 2020 Epson America, Inc. 9/20 CPD-57178

ESPECIFICACIONES COLUMBO

Soporte OS & Requisitos de Sistema

Soporte OS
- Ediciones Windows Desktop 7, 8, 10, 11
- Linux Kernel 4.0 o más reciente (32/64 bit, ARMv6, ARMv7)
  - Ubuntu 18.04, 20.04 o más reciente
  - Debian 10, 11, o más reciente
- Android 10, 11, 12

CPU
- x86 y x64 1.2 GHz o superior; ARM 1.0 GHz o superior

Memoria
- 512MB o superior

Imágenes & Captura

Tipo de Sensor
- LES

Cámara
- CMOS

Resolución
- 500 ppi

Escala de Grises
- 256 rango dinámico en escala de grises

Tamaño de Imagen
- 400 x 500 píxels

Formatos de Imagen Admitidos
- RAW, JPEG2000, BMP, PNG, WSQ (FBI-aprobado)

Cifrado
- N/A

Certificaciones de Imagen/FBI
- PIV 071006, FIPS 201, FAP 30/Certificado para requisitos de identificación móvil

Velocidad
- Tasa de cuadro por minuto > 10 fps, plana y rolos

Interface API
- Captura de un solo dedo, soporte para múltiples dispositivos/ múltiples subprocesos

Puntuación de Calidad
- NFIQ v1 soportado en todos los OSes y NFIQ2 para Windows

Peso & Dimensiones

Peso del Producto
- 23 gramos / 0.06 lbs

Tamaño del Platen
- 21.5 mm x 26,6 mm / 0,8" x 1,0"

Área de Detección
- 20,3 mm x 25,4 mm / 0,8" x 1,0"

Dimensiones del Ensamblaje del Escáner
- 40,0 mm x 42,9 mm x 8,0 mm / 1,5" x 1,6" x 0,3"

Alimentación y Conectores

Interface
- USB 2.0

Fuente de Alimentación
- USB Host

USB Nivel de Voltaje USB
- 4.4V a 5.25V

Conformidad & Certificaciones

Certificaciones USB
- USB-IF USB.ORG

Conformidad FCC/CE
- FCC Parte 15 (por ANSI C63.4: 2014) Clase B, CSA ICES-003 Clase B, CE Emisiones: EN 55022:2010 Class B, CE Immunity EN 55024:2010/AR:2001/A2:2003, IEC 61000-4-2

Descarga de Aire/Descarga de Contacto
- Em conformidade com IEC 61000-4-2

Seguridad del Equipo
- IEC 60950-1

Material Peligroso
- ROHS Directiva 2002/95/EC

Test de Vibración
- Por MIL-STD-810F (Método 514.5), Categoría 24, Fig.514.5C-17

Temperatura & Humedad

Temperatura Operativa
- -10°C ~ +55°C / 14°F ~ 131°F

Humedad
- 20~95% RH < 40°C / 104°F (sin condensación)

Temperatura de Almacenamiento
- -40°C ~ +80°C / -40°F ~ 176°F

Certificaciones
- MOSIP en conformidad

Superficie & Sistemas

Protección de Ingreso/Agua/Polvo
- IP65 Bisel sellado a la superficie de escaneo

Durabilidad de la Superficie
- MIL-C-675c 4.5010, MIL-STD-810F

Limpieza y Desinfección
- Para limpieza y desinfección adecuadas de los productos IB, visite integratedbiometrics.com/clean

Tiempo Medio Entre Fallos (MTBF)
- Basado en 200 inscripciones completas de un solo dedo por día, el MTBF de Columbo es de 66 años.



CONSORCIO EMDOC
EMDOC
CONSORCIO

Productos
Aplicaciones Móviles
Suministros y Accesorios
Soporte y Controladores
Dónde Comprar
Noticias
Promoción y Aprendizaje
Contáctenos

EOS Rebel T100

Cámaras EOS

Artículos de Productos
Dónde Comprar



CONSORCIO EMDOC

Información General | Características | Especificaciones
Contenido de la Caja | Software Actualizado | Servicio y Soporte
Controladores y Software | Folletos y Manuales | Preguntas Frecuentes

Especificaciones

Tipo
Cámara digital réflex de objetivo con Autofoco por fase integrado

Medios de grabación
Tarjetas de memoria SD, SDHC y SDXC

Formato de imagen
Aprox. 22.3 mm x 14.9 mm

Lentes compatibles
Lentes EF de Canon (no incluyen las lentes EF-S y de inclinación y desplazamiento (TS-E))

Estabilizador
Monitor EF-S de Canon

Resolución de imagen

Tipo
Sensor CMOS (aprox. 22.3 mm x 14.9 mm)

Píxeles
Aprox. 18.7 megapíxeles (se redondean a la centena de millón más cercana)

Tamaño de píxel
Aprox. 4.30 µm cuadrados

Total de píxeles
Aprox. 19.0 megapíxeles (se redondean a la centena de millón más cercana)

Relación de aspecto
3:2 (Horizontal:Vertical)

Sistema de filtro de color
Filtro de colores primarios RGB

Filtro de paso bajo
Integrado/fijo

Característica de limpieza de polvo
Limpieza manual y obtención de datos de eliminación de polvo

Sistema de grabación

Formato de grabación
Diseño conforme al estándar de almacenamiento de archivos de cámara (Exif 2.3)

Nombre del archivo
JPEG, Raw (RAW) o Raw + JPEG, original de Canon

Tamaño de archivo
Proporción de aspecto 3:2
Grande: 5184 x 3456
Mediana: 3456 x 2304
Pequeña 1: 2592 x 1728
Pequeña 2: 1920 x 1280
Pequeña 3: 720 x 480
RAW: 5184 x 3456

Proporción de aspecto 4:3
Grande: 4608 x 3456
Mediana: 3072 x 2304
Pequeña 1: 2304 x 1728
Pequeña 2: 1696 x 1280
Pequeña 3: 640 x 480
RAW: 5184 x 3456

Proporción de aspecto 16:9
Grande: 5184 x 2912
Mediana: 3456 x 1944
Pequeña 1: 2592 x 1456
Pequeña 2: 1920 x 1080
Pequeña 3: 720 x 400
RAW: 5184 x 3456

Proporción de aspecto 1:1

CONSORCIO EMDOC
Santo Domingo, D.R.

Grande: 3456 x 3456
Mediana: 2304 x 2304
Pequeña 1: 1728 x 1728
Pequeña 2: 1280 x 1280
Pequeña 3: 480 x 480
RAW: 5184 x 3456

a. Las dimensiones no admitidas se irán teniendo aspecto pedido.

Los ajustes se redondearán a la centena de multiplo cercano. (Para la 5d, los valores se redondean a la decena de mas cada dimensión.)
Las imágenes JPEG se generan según la relación de aspecto seleccionada.
Las imágenes RAW se generan en 3:2 y se ignora la relación de aspecto fijada.

Nombre de archivo
Se pueden configurar los siguientes tres ajustes de numeración de archivos:

1. Numeración continua:
   La numeración de las imágenes sigue incluso si extraes la tarjeta. (La numeración continua incluso cuando cambias tarjeta.)
2. Reinicio automático
   Cuando reconoces la tarjeta de la cámara se reinicia la numeración y comienza a partir de 0001. Si la nueva tarjeta ya contiene imágenes, la numeración comienza a partir de la última imagen grabada en la tarjeta.
3. REINICIO MANUAL
   Finalidad el número del archivo a 0001 y crea automáticamente una carpeta nueva.

Espacio del color
sRGB, Adobe RGB

Estilo de fotografía

- Automático
- Estándar
- Retrato
- Paisaje
- Intenso
- Neutro
- Monocromático
- Definido por el usuario de 1 a 3

Balance de blancos

Balance de blancos automático
Opciones para ambientes en el ambiente y la escena en el balance de blancos.

Configuraciones

1. Automático (Prioridad en el ambiente/Prioridad en el balance de blancos)
2. Luz de día
3. Sombra
4. Nublado
5. Luz de tungsteno
6. Luz blanca fluorescente
7. Flash
8. Personalizado (aprox. 2,000 K – 10,000 K)

Compensación de la temperatura del color
Polarización azul/ámbar: ±9 niveles
Polarización magenta/verde: ±9 niveles
Corrección según la temperatura de color en modo personalizado de balance de blancos.

Visor

Tipo
Pentaespejo

Cobertura
Aprox. 98% vertical / Horizontal (aprox. x 21 mm de ojo)

Ampliación
Aprox. 0.85x (con lente de 50 mm a infinito, -1m⁻¹ dpt)

Punto de ojo
Aprox. 21 mm (desde el centro ocular central)

Corrección del ajuste dióptrico
Rango: -3 a +1 (dpt)
·Se pueden emplear los lentes de ajuste de dioptrías de la serie E para hacer ajustes.

Espejo
Modo espejo de retorno rápido

Información en visor
Punto de AF, indicador de activación de punto de AF, velocidad ISO, compensación de balance de blancos, indicador de enfoque, velocidad ISO, indicador de nivel de exposición, pantalla de ensayo

Vista previa de la profundidad de campo
Si, asignado al botón CONFIGURAR

CONSORCIO EMDOC
EMDOC
22 MAR 2022
DE DERECHO PRIVADO

Enfoque Automático

Tipo
Sistema de detección de fase diferencia de color en la formación de imagen apoyado en TTL con sensor dedicado para AF

Puntos de AF
61 puntos Todos los puntos de AF son compatibles con f/5.6 AF de tipo cruz con punto de AF central

Rango de operación del Enfoque Automático (AF)
Punto de AF central: EV 0–18 (a temperatura ambiente a ISO 100) Otros puntos de AF: EV 1–18 (a temperatura ambiente a ISO 100)

Modos de enfoque

1. Autoenfoque
   a. AF de Servo AI
   b. AF Servo AI Predecible
   c. AF de enfoque AI:
   - Cambia entre AF de Una Toma y AI Servo AF según la escena
2. Enfoque manual

Selección del punto de AF

1. Mediante el dispositivo:
   - Selección automática de 61 puntos
   - Selección manual
2. Mediante el Modo de Control en Vivo:
   - FlexiZone: 1 punto de AF de pequeña o gran selección
   - Modo de Control en Vivo: Selección automática con detección de rostros

Resaltado del punto de AF seleccionado
Iluminado mediante el dispositivo de enfoque automático en el visor y en la pantalla LCD.

Luz de ayuda de AF
Disparo de destello externo de forma manual o cuando un flash Canon EX dedicado cuenta con la función de luz de ayuda de AF (aprox. 4,0 m)

Control de exposición

Modos de medición

1. Mediante el visor óptico:
   - Evaluativa: medición en sensor de medición de doble capa con el área dividida en 63 zonas (vinculado a todos los puntos de AF)
   - Parcial (aprox. el 9% del visor)
   - Está disponible la medición con promedio ponderado en el centro
2. Mediante el modo de control en vivo en la pantalla LCD:
   - Medición evaluativa (315 zonas)

No se admite la medición puntual.

Rango de medición

- Mediante el visor óptico: EV 1–20 (temperatura ambiente, ISO 100, medición evaluativa)
- Mediante el Modo de Control en Vivo en la pantalla LCD: EV 0–20 (a temperatura ambiente, ISO 100, medición evaluativa)

Rango de sensibilidad ISO
Velocidad ISO manual: ISO 100–6400 (en incrementos de 1/3 EV completos), se puede ajustar a una sensibilidad de ISO 12800.
Si se configura la prioridad en tonos de alta luminosidad, la velocidad ISO se configura automáticamente entre ISO 320 e ISO 6400.
Configuración de la velocidad ISO: ISO 800–6400
En los modos de la Zona Creativa, puede configurarse la velocidad ISO máxima (ISO 400, 800, 1600, 3200 o 6400) para ISO automático.[1]

Compensación de la exposición
Manual: EV ±5 en incrementos de 1/3 o 1/2 de paso (se puede combinar con AEB).

Horquillado

- Modos: Modo sin Parpadeo de Escena, Creativo automático, Retrato, Paisaje, Primer Plano, Deportes, Comida, Retrato nocturno, Programa AE, AE con prioridad en el obturador, AE con prioridad en la apertura, Manual, Modos de la Zona Básica
- Estilos de Imagen: Automático, Estándar, Retrato, Paisaje, Neutral, Fiel, monocromáticos, Definido por el usuario (×3)
- Procesamiento de imagen: Prioridad en Tonos de Alta Luminosidad, Optimizador Automático de Iluminación (4 configuraciones), Reducción del ruido en las exposiciones largas, Reducción del ruido (4 configuraciones), Corrección automática de la iluminación periférica (se pueden registrar hasta 20 perfiles en jpeg)
- Filtros creativos: (3D) Grainpaint, Enfoque Suave, Efecto Cámara de Juguete, Efecto Miniatura, Efecto Ojo de Pez, durante la reproducción de imágenes capturadas
- Modos de Manejo: Sencillo, Continuo, Temporizador Automático (2 s, 10 s, 10 s + tomas continuas de 2 a 10)
- Tomas Continuas: Máx. Aprox. 3 fps en JPEG hasta que la tarjeta de memoria se llene.[2] 6 imágenes Raw.[3,4]

Obturador de AE

CONSORCIO EMDOC

- Bloqueado cuando el botón del obturador se presiona hasta la mitad en el modo AF de un [illegible]. Se puede personalizar con el botón de bloqueo AE

Obturador

Tipo
Obturador de plano focal, controlado electrónicamente con primera cortina mecánica

Velocidades de obturación
De 30 a 1/4000 s (se incrementan de en 1/3 o 1/2 de pasos), Exposición Prolongada (Bulb) (Rango total de la velocidad del obturador. Ellevegu Ja puede variar según el modo de uma).

Liberación del obturador
Liberación electromagnética mediante botón de

Auto temporizador
2s, 10s, 20s + toma continua de 3 a 10

Flash integrado

Tipo
Flash integrado

Sistema de control del flash
Flash [illegible] E-TTL II (Evaluativo), Promedio E-TTL, Bloqueo de FE

Número de guía
Aproximadamente 10.2 m/33.2 ft (en ISO 100)

Tiempo de recarga
Aprox. 4 segundos

Cobertura del flash
Ángulo aprox. 17 mm de longitud focal recortable a aprox. 28 mm en formato de 35 mm)

Bloqueo de FE
Posible

Compensación de la exposición con flash
Hasta ±2 pasos en incrementos de 1/3 o 1/2.
La compensación de la exposición con flash en el flash integrado y el flash externo Speedlite se puede configurar con la misma.

Flash Speedlite externo

Compensación de la exposición con flash
±2 pasos en incrementos de 1/3 o 1/2

Configuración del flash externo
E-TTL II con ajuste Speedlite de la cámara

Sistema de enfoque

Modos de enfoque

1. Una toma
2. Toma continua
   - Aprox. 3 fps/auto.
   - Velocidad del obturador 30-1/4000 segundo

Velocidad de toma continua
Aprox. 3.0 fps máx.

Funciones de la vista en vivo

Modos de toma
Toma de fotografías y grabación de vídeo

Enfoque

- Modo de Cpdtg) se Vivo: AF de una toma (AF de detección de contraste)
- Modo Rápido: AF de una toma (versión AF de duración de toma)
- Manual (Ampliación de 5x o 10x disponible)

Modos de medición

- Medición evaluativa (TTL toma)

En posición el bloqueo de AE
- Auto: En el modo AF de una toma por la medición evaluativa, el bloqueo de exposición se fija a cada vez que se toma una foto.
- Manual: Mediante el control de bloqueo de AE en los modos de zona básica

Rango de medición
EV aprox. 0 a 20 (con [illegible] temperatura, a ISO 100)

CONSORCIO EMDOC
EMDOC
Santo Domingo, RD

[illegible] de Hápidos
Rápido (vista previa (x2), histograma

Toma de vídeo

Formato de archivo
MOV
Vídeo: MPEG4 AVC/H.264
Optimizado de [illegible]

Perfil: PCM/Linear

Tamaño de imagen
Full HD
1920 x 1080 (50i) (50p) (24p) (25p) (30p)

HD
1280 x 720 (50p) (60p) (30p) 30 Mbit/s

VGA
640 x 480 (50i) (60i) 20 Mbit/s

Velocidades de los fotogramas
1920 x 1080 (Full HD): 25 fps (29,97 fps)/24 fps (23,98 fps);
1280 x 720 (HD): 50 fps (59,94 fps);
640 x 480 (VGA): 50 fps (29,97 fps)

Enfoque

- AF de cualidad

Sensibilidad ISO
- AUTO (100-6400), ISO 100-6400 en incrementos de 1 paso, se puede ampliar a H: 12800
- Durante la toma de vídeo: AUTO (100-6400), 100-6400 (incrementos de un paso cuando)

Compensación de la exposición
+/-5 EV en incrementos de 1/3 o 1/2 de paso (no puede combinarse con AEB).

Pantalla LCD

Tipo
Pantalla TFT en color, de cristal líquido

Tamaño de la Pantalla
3 pulgadas

Aprox. 6,4 cm (diagonal [illegible]): aprox. 1,1 cm, altura aprox. 4,3 cm)

Píxeles
Aprox. 230.000 puntos

Cobertura
Aprox. 100% vertical y 100% horizontalmente

Control de brillo
Se puede personalizar a uno de cinco niveles de brillo

Idiomas de la interfaz
25 (inglés, [illegible], francés, neerlandés, danés, portugués, finlandés, italiano, noruego, sueco, español, griego, ruso, polaco, húngaro, checo, rumano, ucraniano, árabe, persa, [illegible], coreano, chino simplificado, chino tradicional, japonés, [illegible])

Reproducción

Formato de fotografía

1. Visualización de pre-imagen
   - Información básica
   - Información básica + calidad de imagen + [illegible] de ajuste de imagen
   - Información de cerca
   - Visualización de histograma
2. Visualización de índice: 4 o 9 imágenes
3. Visualización de [illegible] (1/10/100 imágenes por fecha, por carpeta, vídeos solamente, fotografías solamente, no [illegible])

Alerta de obturador
Emite vibraciones en la visualización de la luz y del histograma. los áreas resaltadas en el ajuste de imagen disponible

Función de Control Rápido

Durante la toma
Cuando presiona el botón de Control Rápido mientras dispara en [illegible], puede configurar estas funciones.
Las funciones que se pueden configurar varían según el modo de disparo actual con el modo de Control de Vídeo Total y Guías de Vídeo.

CONSORCIO EMDOC
EMDOC
CONSORCIO EMDOC

Cuando presiona el botón de Control Rápido durante la reproducción, puede establecer estas funciones.
Las funciones que se pueden configurar varían según el tipo de imagen y los ajustes de la cámara.

Protección y borrado de imágenes

Protección
Se puede alternar entre la protección de borrado para una imagen, todas las imágenes en una carpeta o todas las imágenes en la tarjeta.

Borrado
Borra imágenes no protegidas seleccionando la opción de una sola imagen. Imágenes seleccionadas, todas las imágenes en una carpeta o todas las imágenes en la tarjeta.

Impresión Directa

Impresoras compatibles
Impresoras compatibles con PictBridge

Imágenes que se pueden imprimir
Imágenes JPEG y JPEG que cumplan con el "Reglamento de diseño para el Sistema de archivo de Cámaras (DCF, por sus siglas en inglés)" no se pueden imprimir videos.

DPOF: Formato de orden de impresión digital

DPOF
Se admite la creación de órdenes de impresión en formato DPOF (compatible con versión 1.1 y 1.0 DPOF).

Personalización

Funciones Personalizadas
10 funciones personalizadas

Controles Personalizados
No suministrado

Configuración del usuario de la cámara
No suministrado

Registro de "My Menu"
(1) Menú de Toma (M)
(2) Menú de Reproducción (02)
(3) Menú de Configuración (03)
(4) Mi Menú

Interfaz

Terminal USB
Hi-Speed USB equivalente

- Computadora
- PictBridge

Terminal de salida de video
HDMI Tipo D (la resolución cambia automáticamente)
Salida de video: (Compatible automáticamente a 1, 2, 3 o 4 para adaptarse al dispositivo conectado.)

Wi-Fi® (LAN inalámbrica) y funciones de NFC

Comunicación con un teléfono

- Wi-Fi (IEEE802.11b/g/n, 2.4 GHz solamente)
- La conectividad con dispositivos inteligentes se facilita a través de la aplicación Olympus Connect de Canon

Rango de transmisión
Aprox. 49.21 pies/15 m

- Comunicación sin retraso con un teléfono inteligente o tableta.
- Se evita la interferencia de la cámara y un mal funcionamiento debido a otros dispositivos.

Método de conexión

1. Modo de punto de acceso de la cámara (WPA2-PSK con encriptación AES o abierta)
2. Modo de infraestructura (Sólo compatible con encriptación WEP, WPA-PSK/WPA2-PSK con encriptación TKIP/AES o abierta)

Conexión NFC
No está disponible para esta cámara

Fuentes de entrada

CONSORCIO EMDOC

[illegible]
Baterías (LP-E6)

La cámara se puede activar mediante el conector de corriente directa usando accesorios [illegible] con conector de corriente (se venden por separado).

Carga de la batería
Aprox. 595 to 27 °C AE 60%, FE 50%) * Aprox. 640 (0 °C, AE 50%, FE 50%)

Duración de la batería
Verificación automática del nivel de la batería cuando se activa la energía.
El nivel de la batería se indica en uno de los cuatro niveles en la pantalla LCD.

Ahorro de energía
La energía se desactiva después de que transcurra el tiempo de operación establecido.

La configuración de Desactivación Automática de Energía (Auto power off) se puede configurar en 30 s, 1 min, 2 min, 4 min, 8 min, 15 min o Inhabilitado.

Tiempo de inicio
Aprox. 0.1 segundos (basado en las especificaciones de Canon)

Dimensiones y Peso

Dimensiones (An. x Al. x Pr.)
Aprox. 5.78 x 3.88 x 3.63 pulgadas/146.7 x 98.6 x 92.1 mm

- Cumple con los estándares de CIPA.

Peso
Aprox. 18.35 oz/520 g (incluye la batería y la tarjeta)

Entorno de operación

Rango de la temperatura de trabajo
De 32 a 104 °F/de 0 a 40 °C

Rango de la humedad de trabajo
85% o menos

1. Los modos inalámbricos disponibles dependen de la configuración regional. Wi-Fi no está disponible en algunas regiones.

2. Resoluciones grandes (L) y pequeña (S).

3. Basado en las condiciones de prueba de Canon, JPEG, ISO 100, Estilo de imagen Estándar, Varía de acuerdo con el sujeto, la capacidad y formato de la tarjeta de memoria, la configuración de imagen, la velocidad ISO, el modo de disparo, el Estilo de Imagen, las funciones Personalizadas, etc.

4. La prueba de la velocidad de toma continua se basa en las condiciones de prueba de Canon. La función requiere una tarjeta de memoria compatible con UHS-I de velocidad clase 3 o superior. Los resultados varían según la toma, las configuraciones y la marca de la tarjeta de memoria.

5. No se puede utilizar una tarjeta de Eye-Fi para cargar los archivos (incluso cuando esta función está deshabilitada). Verifique los términos de los archivos con el fabricante de la tarjeta.

6. Modos de operación inalámbrica.

7. El proceso de uso del Wi-Fi está restringido en algunos países o regiones.

8. La aplicación Camera Connect de Canon está disponible para los dispositivos Apple iOS y Android compatibles. Visite Google Play Store™ y Apple App Store para conocer las versiones compatibles de Android OS y Apple iOS.

9. Basado en el establecimiento de CIPA, con el uso de las baterías y la cámara se trabaja en ambientes ambientales con la cámara a [illegible] grados centígrados.

[illegible]

[illegible]

* Compatible con las versiones 8.3/8.3.1/8.4 de iOS® con los sistemas inteligentes y cámaras Android™ en las versiones 4.4/5.0/5.1/6.0/7.0/7.1/8.0 o posterior que cumplan con los [illegible] de la tecnología de comunicación cercana Camera Connect de Canon. Esta aplicación no admite ciertos teléfonos inteligentes fuera de nuestro mercado. Tenga en cuenta que los sistemas inteligentes pueden cambiar. Información de compatibilidad actualizada puede [illegible] Canon no obtiene, acepta ni otorga responsabilidad por la información [illegible] inteligentes, incluyendo esta aplicación.

* Compatible con los teléfonos inteligentes y tabletas Android™ en las versiones 4.4.2/5.0/5.1/6.0/7.0/7.1/8.0.

Todos los datos deben basarse en los métodos de prueba estándar de Canon, a menos donde se indica.

[illegible] compatible con [illegible]

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

2 de 2

CC eIDAS en CryptoServer HSM de propósito general

utimaco®

Dispositivo cualificado de creación de firmas (QSCD) conforme con eIDAS y con certificación CC

Firmas y sellos compatibles con eIDAS* Firma de servidor eIDAS* Protección de claves* Certificado CC* Simulador incluido

La versión de conformidad CC eIDAS para CryptoServer General Purpose HSM ayuda a los proveedores de servicios de confianza (TSP) a cumplir los requisitos de política y seguridad definidos en varias normas técnicas del ETSI (ETSI EN 319 401, EN 319 411, EN 319 421).

Casos clave



CC eIDAS on CryptoServer General Purpose HSM está diseñado específicamente para firmas y sellos cualificados compatibles con eIDAS, firma remota y emisión de certificados cualificados.

Aspectos destacados

- Firma cualificada / Dispositivo de creación de sellos
- Firma de servidores eIDAS
- Hardware realsterio protección
- Cumple diversos mandatos de conformidad
- Simulador de software incluido

Principales ventajas

Dispositivo cualificado de creación de firmas y sellos (QSigCD y QSealCD)

CC eIDAS que se ejecuta en CryptoServer ha recibido la certificación eIDAS como Dispositivo Cualificado de Firma y Creación de Sello (QSCD) y puede utilizarse como QSCD independiente o como parte de un QSCD combinado con soluciones de firma remota.

Módulo de activación de firmas (SAM) listo para la firma de servidores eIDAS

Utilizando un producto complementario, el CryptoServer SDK, para el desarrollo de un módulo de activación de firma (SAM), que se ejecuta dentro del límite certificado del HSM.

Sólida protección de activos sensibles mediante hardware

Una raíz de confianza segura para almacenar activos sensibles como claves privadas y datos y, opcionalmente, ser gestionada como un "QSCD remoto" por un proveedor de servicios de confianza cualificado (QTSP).

Cumple diversos mandatos de conformidad

CC eIDAS on CryptoServer General Purpose HSM cuenta con la certificación Common Criteria EAL4+ de acuerdo con el Perfil de Protección EN 419 221-5, así como con los puntos 23 y 32 del artículo 2 del Reglamento 910/2014 (eIDAS). También permite Server Signing según EN 419 241-2 y cumple los requisitos de política y seguridad del ETSI (por ejemplo, EN 319 401, EN 319 411, EN 319 421, CITS).

Simulador HSM con todas las funciones

Pruebas antes de la implantación: El simulador totalmente funcional permite realizar pruebas de integración al ofrecer un tiempo de ejecución completamente funcional, incluida la administración y la gestión de la configuración.

CONSORCIO EMDOC
EMDOC
Santo Domingo, RD

462-2

Funciones de gestión de HSM

- Amplia gestión de claves con autorización de claves
- API y herramienta de autorización de claves (según PP EN 419 221-5)
- autenticación de quórum "m de n" (por ejemplo, 3 de 5)
- Autenticación de dos factores con tarjetas inteligentes
- Control de acceso configurable basado en funciones y separación de tareas
- Soporte multi-tenancy
- Gestión y administración remotas
- Sistemas operativos compatibles: Windows y Linux
- Múltiples integraciones con aplicaciones PKI, etc.
- Gestión eficaz de claves y actualizaciones de firmware mediante acceso remoto
- Automatización del diagnóstico remoto mediante SNMP (protocolo simple de gestión de redes)

Algoritmos criptográficos

- RSA, ECDSA con curvas NIST y Brainpool
- ECDH con curvas NIST y Brainpool
- AES
- CMAC, HMAC
- Familia SHA2, SHA3
- Generador de números aleatorios determinista basado en hash (DRG.4 según AIS 31)
- Generador real de números aleatorios (PTG.2 según AIS 31)
- Hasta 3.000 operaciones de firma RSA o 2.500 ECDSA en modo de procesamiento masivo
- Todos los algoritmos incluidos en el precio del producto

Interfaces de programación de aplicaciones (API)

- PKCS #11
- Criptografía de próxima generación (CNG)
- Cryptographic eXtended services Interface (CXI) -La interfaz de alto rendimiento de Utimaco garantiza fácil integración de las funciones criptográficas en las aplicaciones cliente

Hardware

Dispositivo de red



Tarjeta PCIe



Dimensiones físicas

Factor de forma	19" 1U	De medio cuerpo, tarjeta PCI Express de altura completa y un solo carril
Peso	22,05 lb (10 kg)	0,55 lb (0,4 kg)
Talla	W 17,56 in × D 21,73 in × H 1,73 in (W 446 mm × D 533,4 mm× H 44 mm) sin cerraderas	W 4,38 in× D 6,89 in × H 0,74 in (W 111,15 mm × D 187,65 mm× H 18,6 mm)

Conectividad

Interfaces	2 RJ45, 1 Gb/s	USB

Características eléctricas

Fuente de alimentación / batería	Reemplazable en campo redundante, 2 x 100 ~ 240 V CA, 50 ~ 60 Hertz, 300 W	Batería de reserva: Batería de litio de 3 V, Ø 12 mm, longitud 10 mm, FDK CR 1/2600 SE o VARTA CR2NP
Consumo / Tensión de funcionamiento	Normalmente 45 W / 66 VA, máx. 50 W / 70 VA	3,3 V
Calor	Disipación de calor: máx. 171 BTU/h	

Entorno operativo

Temperatura de funcionamiento	De +50°F a +122°F (de +10°C a +50°C)	De +50°F a +113°F (de +10°C a +45°C)
Humedad relativa de funcionamiento	Del 10% al 85%, sin condensación	Del 15% al 85%, sin condensación
Temperatura de almacenamiento	De +14°F a +131°F (de -10°C a +55°C)	De +14°F a +131°F (de -10°C a +55°C)
MTBF	100.000 horas a 25°C / 77°F, Medio ambiente GB, GC - Suelo Benigno, Controlado	360.000 horas a 25°C / 77°F

Certificación / Conformidad

	IEC/EN 60950-1, IEC/EN 62368-1, UL, Certificado CB, CE, FCC Clase B Medioambiental: RoHS III, WEEE Seguridad: FIPS 140-2 Nivel 3

EMEA

Utimaco IS GmbH

Germanusstrasse 4
52080 Aachen,
Alemania

+49 241 1696 200
info@utimaco.com

América

Utimaco Inc.

Suite 400
910 E Hamilton Ave.,
Campbell, CA 95008,
EE.UU.

+1 844 UTIMACO
info@utimaco.com

APAC

Utimaco IS Pte Limited

6 Temasek Boulevard
#23-04 Suntec Tower Four
Singapur 038986

+65 6993 8918
info@utimaco.com

Para más información sobre los productos Utimaco®, visite:
utimaco.com

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

utimaco®

© Utimaco IS GmbH 09/24 - Versión 5.0

Utimaco® es una marca comercial de Utimaco GmbH. Todas las demás marcas mencionadas son marcas registradas del titular de los derechos de autor. Todos los derechos reservados. Las especificaciones están sujetas a cambios sin previo aviso.

Lector de tarjetas RFID

Lector de 13.56Mhz con soporte ISO14443-A / B, protocolo de tarjeta IC Lector IC de tarjeta sin contacto

Características Generales

- Interfaz USB: No se necesita una fuente de alimentación externa, Plug in and Play, por lo que no necesita controlador, solo conecte USB a su teléfono inteligente o comunicador, lea el número de tarjeta.
- Fuerte compatibilidad: Compatible con múltiples sistemas, Windows / Linux / Android / Mac OS.
- Aplicaciones: Tarjeta MF S50 S70 tarjeta bancaria y otras etiquetas de protocolo 14443A que admiten el protocolo ISO14443-A / B, tarjeta de identificación y otras etiquetas de protocolo 14443B.
- Estado de funcionamiento: el rojo indica el modo de espera y el verde indica que la tarjeta se ha deslizado correctamente.
- Frecuencia de trabajo: 13.56MHZ



Características y Especificaciones

Tipo de medio admitido	MultipleFileTypes
Tecnología de conectividad	USB, USB Tipo C, USB Tipo A
Características adicionales	Plug & Play
Dispositivos compatibles	Teléfono inteligente
Sistema operativo	Linux, Windows XP
Conectividad de hardware	USB

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

464

VOTAN

Método de uso



1. Conecte el lector en el puerto USB



2. Abra una aplicación como Notepad o Word



3. Coloque la tarjeta sobre el lector

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

464-1
Ficha técnica

FortiADC™

Controlador avanzado de entrega de aplicaciones

Disponible en:





Destacados

- Avanzado L4-L7 Aplicación LB
- La integración en la nube de FortiGSLB maximiza la disponibilidad del servicio
- AL (Aprendizaje Adaptativo), y OWASP Top-10 protección y conformidad con cortafuegos de aplicaciones web
- Modo de despliegue múltiple con proveedores de hardware, VM, FortiFlex o Cloud (PAYG/BYOL)
- Seguridad y visibilidad SSL con una solución basada en hardware
- Conector de automatización y tejido a soluciones de terceros como K8s y OCP Ingress Controller, SAP, AWA y OCI
- Autenticación y autorización de usuarios mediante MFA y SSO
- Aplicación en cualquier lugar con servidor global LB

Entrega de aplicaciones con seguridad y optimización

En los últimos años, el panorama de la entrega de aplicaciones ha experimentado importantes transformaciones influidas por la evolución de las tendencias tecnológicas y la creciente adopción de la computación en nube. Muchas organizaciones están integrando centros de datos locales con entornos de nube pública para optimizar el rendimiento de las aplicaciones, aumentar la escalabilidad y mejorar la agilidad general del negocio.

Introducción

FortiADC, el avanzado Application Delivery Controller (ADC), optimiza la entrega de aplicaciones, mejora el rendimiento y garantiza la seguridad de las aplicaciones, ya estén alojados en las instalaciones o en la nube.

FortiADC ofrece sólidas capacidades de equilibrio de carga L4-L7 con soporte Scripting para manipulación de contenidos y Servicios Avanzados SSL (Offloading y mirroring).

FortiADC también ofrece aceleración de aplicaciones, autenticación y funciones de seguridad integradas, como protección Web Application Firewall para cualquier amenaza de aplicación AL (Adaptive Learning), y OWASP Top10 Compliance Policy), protección DDoS, ZTNA y mucho más.

Con opciones de despliegue flexibles (HW, VM, FortiFlex y Cloud Providers) e integración en Fortinet Security Fabric, FortiADC permite a las empresas ofrecer experiencias de aplicación y seguridad excepcionales.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

Descripción general de FortiADC



Destacados

Disponibilidad de solicitudes

Las aplicaciones son el alma de la presencia en línea de una empresa. Las aplicaciones que no responden pueden provocar pérdidas de ingresos y que los clientes se vayan a hacer negocios a otra parte. El rendimiento, la escalabilidad y la resistencia de las aplicaciones son fundamentales, pero nada de esto importa a menos que el usuario final tenga una buena experiencia y complete su transacción.

FortiADC es una solución dedicada de Application Delivery Control que proporciona una solución multi-tenancy (VDOM y ADOM), alta disponibilidad y escalabilidad con despliegue de solución híbrida (on-premises y oferta cloud) para sus aplicaciones.

Protección de aplicaciones web

FortiADC Web Application Firewall (WAF) proporciona una solución de seguridad integral diseñada para proteger las aplicaciones web de una amplia gama de amenazas. Nuestro WAF incluye características robustas como AL (Aprendizaje Adaptativo), que analiza dinámicamente el tráfico de clientes y servidores para construir políticas en tiempo real para bloquear ataques web. Además del aprendizaje adaptativo, FortiADC WAF ofrece amplias firmas WAF, que garantizan la protección frente a las 10 principales vulnerabilidades OWASP. También incluye seguridad avanzada de API y protección contra ataques de relleno de credenciales, ofreciendo un enfoque holístico e inteligente de la seguridad de las aplicaciones.

Aplicación en cualquier lugar (GSLB)

El módulo FortiADC incluido Global Server Load Balancing (GSLB) on prem o en la nube (FortiGSLB Cloud) hace que su red sea fiable y disponible mediante el escalado de aplicaciones a través de múltiples centros de datos para la recuperación de desastres o para mejorar los tiempos de respuesta de las aplicaciones. Los clientes pueden configurar reglas basadas en la disponibilidad del sitio, el rendimiento del centro de datos y la latencia de la red.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

Hechos destacados

Optimización de datos



FortiADC proporciona múltiples servicios que aceleran la entrega de aplicaciones a los usuarios. La suite PageSpeed de herramientas de mejora del rendimiento de sitios web puede optimizar automáticamente la entrega de HTTP, CSS, Javascript e imágenes a los usuarios de las aplicaciones. FortiADC también proporciona almacenamiento en caché dinámico y compresión y descompresión HTTP para mejorar la experiencia del usuario final y la productividad del servidor.

Gestión del acceso a las aplicaciones



FortiADC proporciona servicios centralizados de autenticación y autorización de usuarios para aplicaciones web. FortiADC actúa como gatekeeper para descargar la autenticación y autorización HTTP a las aplicaciones del cliente mediante servicios de inicio de sesión único (SSO), SAML, LDAP, RADIUS y MFA (mediante FortiToken Cloud y Google authenticator).

Seguridad AI

FortiADC ahora soporta seguridad AI con Threat Analytics y FortiGuard Advanced Bot Protection.



- Threat Analytics evalúa continuamente su postura de seguridad supervisando los ataques a sus activos web y evaluando su configuración de WAF y Seguridad y, basándose en los Insights, proporciona acciones recomendadas que pueden mejorar sus ajustes de configuración de WAF y Seguridad, bloquear futuros ataques y reducir los falsos positivos.



- FortiGuard Advanced Bot Protection es una defensa integral contra la amenaza siempre presente de los bots. Proporciona una solución SaaS de vanguardia para proteger sus aplicaciones web y activos digitales de la amenaza en constante evolución de los bots utilizando telemetría de cliente y servidor y aprendizaje profundo.

Características principales

Servicios avanzados de seguridad



A medida que evoluciona el panorama de las amenazas, muchos riesgos nuevos requieren un enfoque múltiple para proteger las aplicaciones. FortiADC ofrece protecciones multivectoriales, desde la red (IPS, antivirus, reputación de IP) hasta las aplicaciones (DLP, Sandbox, Credential Stuffing y WAF Signatures), pasando por la seguridad de IA con análisis de amenazas y protección avanzada contra bots.

Descarga SSL y visibilidad



FortiADC ofrece alta capacidad de descifrado y cifrado con el último estándar de criptografía utilizando SSL ASIC basado en hardware. FortiADC proporciona descarga SSL, inspección SSL y visibilidad para inspeccionar el tráfico en busca de amenazas, acelera la respuesta del servidor y reduce la carga en el servidor backend. FortiADC también se integra con el módulo de seguridad de hardware (HSM) SafeNet Enterprise de Gemalto.

Scripts y herramientas DevOps



FortiADC Scripts proporciona la flexibilidad necesaria para crear reglas personalizadas basadas en eventos utilizando comandos, variables y operadores predefinidos. Utilizando scripts fáciles de crear, obtendrá la flexibilidad que necesita para ampliar su FortiADC con una reescritura avanzada de contenidos y decisiones de aplicación. FortiADC también ofrece una gama de herramientas DevOps, como RestfulAPI, Declarative API, Terraform, cloud-init y Ansible, que mejoran la eficiencia del despliegue, la gestión y la automatización de aplicaciones.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

Características principales

Automatización y conectores

FortiADC Fabric Connectors proporciona integración y orquestación abierta basada en API con múltiples redes definidas por software (SDN), cloud, gestión y plataformas tecnológicas de partners. Los Fabric Connectors de Fortinet ofrecen integración llave en mano, abierta y profunda en servicios de terceros como K8s, AWS, OCI y SAP, en ecosistemas de múltiples proveedores, lo que permite escalabilidad, automatización de la seguridad y gestión simplificada.

Análisis y visibilidad

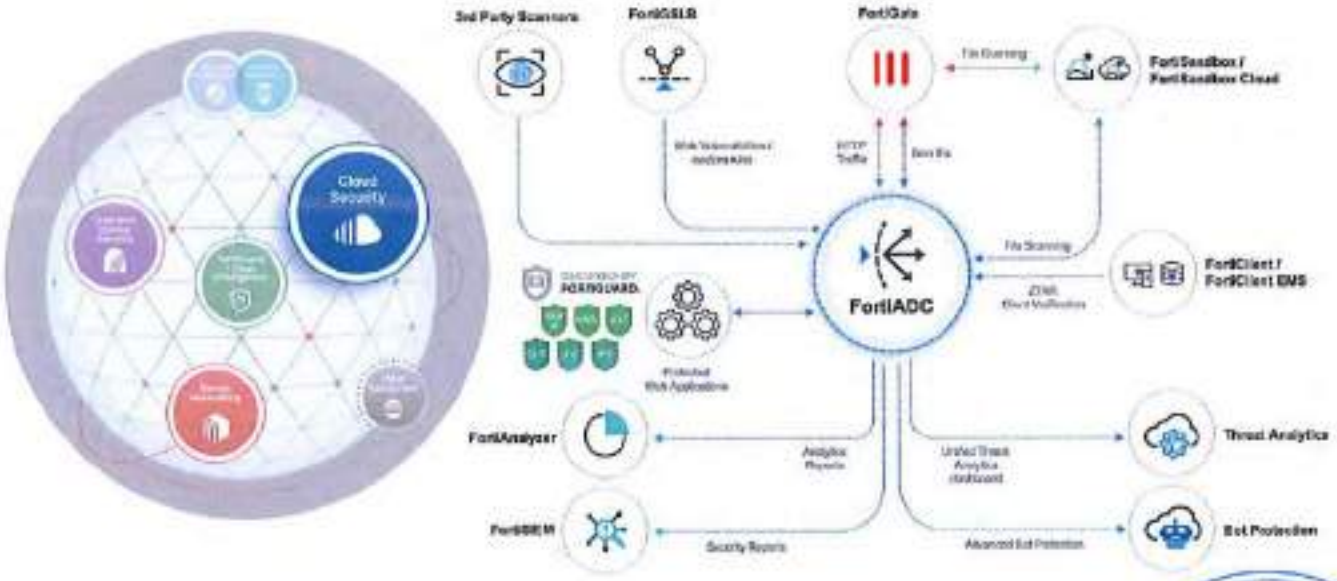
FortiADC ofrece un completo sistema de monitorización para su red y aplicación. Con FortiView, los clientes pueden obtener datos históricos y en tiempo real en una única vista de su . También proporcionamos una topología lógica de red de servidores reales, análisis de datos de usuarios/aplicaciones, amenazas de seguridad, mapas de ataques y algunos otros eventos y alertas del sistema.

FortiADC soporta ADC Manager para gestionar múltiples dispositivos FortiADC de forma remota, y se integra con soluciones de terceros como Splunk, FortiAnalyzer y FortiSIEM para una mayor visibilidad, correlación, respuesta automatizada y remediación.

Conectores de tejido de seguridad

Los conectores de tejido FortiADC integran a la perfección FortiADC con varias soluciones Fortinet Security Fabric, permitiendo procesos automatizados para gestionar actualizaciones dinámicas de seguridad sin intervención manual. Estos conectores definen el tipo de integración y facilitan un ecosistema cohesivo para que los productos de Fortinet trabajen juntos de forma armoniosa.

FortiADC soporta una amplia gama de integración de Tejido de Seguridad con: FortiGate, FortiSIEM, FortiAnalyzer, FortiGSLB, Threat Analytics y FortiGuard Advanced Bot Protection. El objetivo general es mejorar la colaboración y la automatización en toda la suite de productos Fortinet a través de Fabric Connectors.



CONSORCIO EMDOC
EMDOC CONSORCIO
Santo Domingo, RD

Casos prácticos

FortiADC admite múltiples casos de uso para cualquier organización (telecomunicaciones, educación, sanidad, finanzas, etc.).

Descubra los casos de uso clave de FortiADC para su organización:



CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

Experiencia con paquetes FortiADC

Aumentar la seguridad en las redes, las aplicaciones y más allá

Seguridad en las redes



Fortifique su infraestructura frente a cualquier amenaza de red con funciones avanzadas de seguridad de red. Este paquete garantiza una protección sólida, minimiza las vulnerabilidades y salvaguarda la integridad de su red.

Seguridad de las aplicaciones



Proteja sus aplicaciones de posibles ataques con el completo paquete de seguridad de aplicaciones. Beneficiese de defensas personalizadas contra amenazas específicas de las aplicaciones, que garantizan el rendimiento y la fiabilidad ininterrumpidos de sus aplicaciones críticas.

Seguridad AI



Adopte el futuro de la ciberseguridad con el paquete AI Security. Basado en modelos de IA/ML de última generación, este paquete ofrece una defensa proactiva frente a ataques sofisticados. Analiza las amenazas en tiempo real, lo que le permite anticiparse a las ciberamenazas y responder con eficacia.

		Seguridad de las redes	Seguridad de las aplicaciones	AI Seguridad
Seguridad de las redes	Reputación IP y GeoIP	●	●	●
	Protección avanzada contra malware	●	●	●
	Servicio de prevención de intrusiones	●	●	●
Seguridad de las aplicaciones	Firmas WAF y aprendizaje adaptativo		●	●
	Defensa contra la usurpación de credenciales		●	●
	Nube Sandbox		●	●
	FortiGuard DLP		●	●
AI Seguridad	Análisis de amenazas			●
	Protección avanzada contra bots			●

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

Características de FortiADC

CASOS DE USO	FUNCIONES COMPATIBLES
Disponibilidad de solicitudes	Equilibrio de carga L4-L7 avanzado (Aplicación y protocolos)
	Presencia, comprobación avanzada, enrutamiento de contenidos y reescritura
	Soporte de secuencias de comandos y enrutamiento y manipulación de contenidos L7
	Servicios avanzados SSL TLS1.3 (Offloading/Mirroring) y proxy de reenvío SSL
	Gestión SSL ()+ Compatibilidad con Let's Encrypt
Aplicación en cualquier lugar	Equilibrio global de la carga de servidores (geolocalización, RR, peso, etc.)
	Protección Geo-IP y reputación IP
	Seguridad del DNS y DNSSEC
Optimización de aplicaciones	Caché dinámico y compresión
	Velocidad de página HTTP (optimización y multiplexación)
Protección de aplicaciones	Cortafuegos de aplicaciones web y escáner de vulnerabilidades web
	Seguridad de API (OpenAPI, API-GW, API Discovery)
	WAF (AL) Apoyo al aprendizaje adaptativo
	Firma de seguridad de aplicaciones web FortiGuard
	Defensa contra la usurpación de credenciales
	Cumplimiento de la OWASP top-10
	Protección avanzada contra bots
Seguridad de acceso a las aplicaciones	Autenticación de aplicaciones: formulario, básica y SSO
	SAML, Kerberos, Auth2.0, LDAP, RADIUS, FortiToken, Google Auth
	FortiGuard Cloud Sandbox
	Prevención de fuga de datos FortiGuard
Sistemas y redes	Soporte VDOM/ADOM
	NAT completa (1:1, dinámica, estadística y Hide-NAT)
	Alta disponibilidad (VRRP A/A, A/P Failover)
	Compatibilidad con IPv4 e IPv6
	Enrutamiento dinámico (BGP, OSPF) y compatibilidad con NVGRE y VXLAN
Seguridad en las redes	Protección DDoS (redes y aplicaciones)
	Cortafuegos de estado
	Pasarela de aplicaciones de confianza cero
	Prevención de intrusiones FortiGuard
	Protección antimalware (AV) FortiGuard
Análisis de datos y SecOps	FortiView - Análisis de datos
	OWASP top-10 Supervisión en tiempo real
	Informes en tiempo real, supervisión, registro y SNMP
	Análisis de amenazas AI
Integración de Fabric y herramientas DevOps	Integración: SAP, K8s, OCP, AWS, MS (SharePoint, RDP, Exchange), Splunk, Cisco-ACI, etc.
	Security Fabric - FortiGate, FortiSIEM, FortiAnalyzer, FortiClient, FortiAuthenticator, FortiGSLB
	Restful, y Declarative API, Ansible, Terraform, y Cloud-Init
Asistencia Premium 24x7	Asistencia Premium FortiCare

* La disponibilidad de las funciones depende de la suscripción o determinados paquetes de licencias.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

Especificaciones

	[illegible]	[illegible]
[illegible]		
[illegible]	5 Gbps / 4 Gbps	10 Gbps
L4 CPS	160 000	350 000
L4 HTTP RPS	500 000	1,2M
Conexión simultánea L4 máximo	6M	18M
L7 CPS (1:1) *	40 000	120 000
SSL CPS/TPS (1:1) 2K llaves **	1000	4400
Rendimiento del cifrado inverso SSL	1,2 Gbps	3 Gbps
Rendimiento de compresión	2 Gbps	6 Gbps
Tecnología de aceleración SSL	Software	software
Dominios virtuales	10	25
Especificaciones de hardware		
Memoria	8 GB	16 GB
Interfaces de red	4x GE RJ45, 4x GE SFP	2x 10 GE SFP+, 4x GE SFP, 4x GE RJ45
Interfaz de gestión 10/100/1000	-	1
Almacenamiento	120 GB SSD	120 GB SSD
Gestión	HTTPS, SSH CLI, Consola directa DB9 CLI, GUI/API	HTTPS, SSH CLI, Consola directa DB9 CLI, GUI/API
Puertos de almacenamiento	0 bays	0 bays
Puertos virtuales (VR)	10	20
Modo de alta disponibilidad de contenido	Sí	No
Dimensiones		
Altura x Ancho x Longitud (pulgadas)	1,75 x 17,24 x 16,38	1,75 x 17,0 x 15,0
Altura x Ancho x Longitud (mm)	44 x 438 x 416	44,45 x 432 x 380
Peso	6,67 kg (22 lb)	5,5 kg (12 libras)
Medio ambiente		
Factor de forma	Ajustes 1U	Ajustes 1U
Tensión de entrada	100-240 V CA, 50-60 Hz	100-240 V CA, 50-60 Hz
Consumo (media / máximo)	85W	40 W / 60 W
Corriente máxima	100V/5A, 240V/2A	8A / 2A
Fuente de alimentación CC	-	-
Disipación del calor	273 BTU/h	150-183 BTU/h
Temperatura de funcionamiento	5°C a 40°C (32°F a 104°F)	0°C a 40°C (32°F a 104°F)
Temperatura de almacenamiento	-20°C a 70°C (-4°F a 158°F)	-20°C a 70°C (-4°F a 158°F)
Humedad	5% a 95% sin condensación	10% a 85% de humedad relativa, sin operación, sin condensación
Flujo de aire forzado	De delante hacia atrás	De delante hacia atrás
Conformidad		
Cumplimiento de la normativa	FCC Parte 15 Clase A, RCM, VCCI Clase A, CE, UL/A	FCC Parte 15 Clase A, RCM, VCCI Clase A, CE, UL/A
Seguridad	CSA, C/US, CE, UL	CSA, C/US, CE, UL

[illegible]

Todos los valores de rendimiento son "hasta" y varían en función de la configuración del sistema.
** Capa 7 CPS - mide el número de nuevas conexiones HTTP (1 petición HTTP por conexión TCP).
** Probado con 1 petición HTTP por conexión SSL; Cifrado SSL=RSA-AES256-SHA; Claves 2K

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

Especificaciones

	[illegible]	[illegible]
[illegible]		
Rendimiento L4/L7	20 Gbps	40 Gbps / 30 Gbps
L4 CPS	200 000	1 000 000
L4 HTTP RPS	2 M	8 000 000
Conexión simultánea L7 máxima	2 M	50 000 000
L7 CPS (1:1) *	203 000	340 000
SSL CPS/TPS (1:1) 2K llaves **	20 000	35 000
Rendimiento del cifrado masivo SSL	10 Gbps	15 Gbps
Rendimiento de compresión	14 Gbps	28 Gbps
Tecnología de aceleración SSL	ASIC	ASIC
Dominios virtuales	45	45
Especificaciones de hardware		
Memoria	32 GB	32 GB
Interfaces de red	4x 10 GE SFP+, 4x GE SFP, 4x GE RJ45	8 puertos RJ45 GE, 8 puertos SFP GE, 8 puertos SFP+ 10GE
Interfaz de gestión 10/100/1000	2	2
Almacenamiento	120 GB SSD	240 GB SSD
Gestión	HTTPS, SSH CLI, consola directa DB9 CLI, SNMP	HTTPS, SSH CLI, Consola directa DB9 CLI, SNMP
Fuente de alimentación	Redundante (cambio doble, fuente de alimentación intercambiable en caliente)	Doble (cambio fuente de alimentación intercambiable en caliente)
Módulo de plataforma de confianza (TPM)	Sí	Sí
Dimensiones		
Altura x Anchura x Longitud (pulgadas)	17,4 x 19,6 x 9	1,73 x 21,5 x 17,3
Altura x Anchura x Longitud (mm)	44 x 498 x 229	44 x 548 x 440
Peso	6,4 kg (14,11 lb)	10,3 kg (22,5 lbs)
Medio ambiente		
Factor de forma	Aparato 1U	Aparato 1U
Tensión de entrada	100-240 V CA, 50-60 Hz	100-240 V CA, 50-60 Hz
Consumo típico / máximo	89 W / 140 W	231 W / 330 W
Corriente máxima	3A / 1A	100V / 1A, 240V / 1,5A
Fuente de alimentación CC	-	Soporte
Disipación del calor	282 BTU/h	856 BTU/h
Temperatura de funcionamiento	0°C a 40°C (32°F a 104°F)	0°C a 40°C (32°F a 104°F)
Temperatura de almacenamiento	-20°C a 75°C (-4°F a 167°F)	-30°C a 75°C (-4°F a 167°F)
Humedad	10% a 85% de humedad relativa, sin condensar, sin condensación	10% a 85% sin condensación
Hoja de ruido acústico	De dolores hechizante	De dolores hechizante
Conformidad		
Cumplimiento de la normativa	FCC Parte 15 Clase A, RCM, VCCI Clase A, CE, UL/cUL	FCC, CE, RCM, VCCI, BSMI
Seguridad	CSA, C/US, CE, UL	UL/ cUL, CB





Todos los valores de rendimiento son "hasta" y varían en función de la configuración del sistema.
** Capa 7 CPS - mide el número de nuevas conexiones HTTP (1 petición HTTP por conexión TCP).
** Probado con 1 petición HTTP por conexión SSL; Cifrado SSL-RSA-AES256-SHA; Claves 2K.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

Especificaciones

	FortiADC 2000F/2C	FortiADC 4000F/4C	FortiADC 5000F
Rendimiento del sistema			
Rendimiento L4/L7	60 Gbps / 35 Gbps	100 Gbps / 70 Gbps	350 Gbps / 220 Gbps
L4 CPS	1 200 000	1 900 000	4M
L4 HTTP RPS	3 000 000	5 000 000	18 000 000
Conexión simultánea L4 máxima	72 000 000	144 000 000	216 000 000
L7 CPS (1:1) *	360 000	530 000	1 130 000
SSL CPS/TPS (1:1) 2K Bare **	80 000	90 000	96 000
Rendimiento de cifrado masivo SSL	22 Gbps	32 Gbps	300 Gbps
Rendimiento de descompresión	22 Gbps	45 Gbps	150 Gbps
Tecnología de aceleración SSL	ASIC	ASIC	ASIC
Dominios virtuales	60	90	90
Especificaciones de hardware			
Memoria	64 GB	128 GB	384 GB
Interfaces de red	8 SFP, 12 puertos SFP+ 10GbE	4x 40GbE QSFP, 8x 10G SFP+	4x 100 GE QSFP28, 8x 40 GE QSFP
Interfaz de gestión 10/100/1000	2	2	1
Almacenamiento	240 GB SSD	480 GB SSD	1.74 TB SSD
Gestión	HTTPS, SSH CLI, Consola directa DB9 CLI, SNMP	HTTPS, SSH CLI, Consola directa DB9 CLI, SNMP	HTTPS, SSH CLI, Consola directa DB9 CLI, SNMP
Fuente de alimentación	Doble (admite fuente de alimentación intercambiable en caliente)	Doble (admite fuente de alimentación intercambiable en caliente)	Doble (admite fuente de alimentación intercambiable en caliente)
Módulo de plataforma de confianza (TPM)	Sí	Sí	No
Dimensiones			
Altura x Anchura x Longitud (pulgadas)	1,73 x 17,3 x 12,3	3,46 x 17,3 x 17,3	6,4 x 17,2 x 30,3
Altura x Anchura x Longitud (mm)	44 x 548 x 440	88 x 548 x 440	80,6 x 439,9 x 777,1
Peso	10,2 kg (22,5 lbs)	15,3 kg (29,3 lbs)	31 kg (68,5 lbs)
Medio ambiente			
Factor de forma	Montaje 1U	Montaje 2U	Montaje 5U
Tensión de entrada	100-240 V CA, 50-60 Hz	100-240 V CA, 50-60 Hz	220-240 V CA, 50-60 Hz
Consumo (medio / máximo)	161 W / 180 W	269 W / 460 W	1139 W / 1300 W
Corriente máxima	100V / 2A, 240V / 1,5A	100V / 3A, 240V / 1,9A	220V / 6A, 240V / 5A
Fuente de alimentación CC	Soporte	Soporte	-
Disipación del calor	511 BTU/h	912 BTU/h	3500 BTU/hora
Temperatura de funcionamiento	0°C a 40°C (32°F a 104°F)	0°C a 40°C (32°F a 104°F)	10°C a 35°C (50°F a 95°F)
Temperatura de almacenamiento	-25°C a 70°C (-4°F a 158°F)	-20°C a 70°C (-4°F a 158°F)	-40°F a 140°F (-40°C a 60°C)
Humedad	10% a 85% sin condensación	10% a 85% sin condensación	8% a 90% sin condensación
Flujo de aire forzado	De delante hacia atrás	De delante hacia atrás	De delante hacia atrás
Conformidad			
Cumplimiento de las normativas	FCC, CE, RCM, VCCI, BSMI	FCC, CE, RCM, VCCI, BSMI	CE, FCC, RCM, VCCI, BSMI
Seguridad	UL/cUL, CB	UL/cUL, CB	UL, CB, BIS







Todos los valores de rendimiento son "hasta" y varían en función de la configuración del sistema.

** Capa 7 CPS - mide el número de nuevas conexiones HTTP (1 petición HTTP por conexión TCP).

** Probado con 1 petición HTTP por conexión SSL; Cifrado SSL=RSA-AES256-SHA; Claves 2K.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

464 - 11

Especificaciones

	FORTIADC-VM01	FORTIADC-VM02	FORTIADC-VM04	FORTIADC-VM08	FORTIADC-VM16	FORTIADC-VM32
Especificaciones de hardware						
Compatibilidad con hipervisores	VMware ESXi/ESX 5.5, Citrix XenServer, Open Source Xen, Microsoft Hyper-V, KVM, AWS, Azure, Google Cloud, Oracle Cloud, IBM Cloud, Alibaba Cloud, Nutanix y Proxmox. Por favor, consulte la Guía de instalación de FortiADC-VM para conocer las últimas versiones de hipervisor soportadas.					
Rendimiento* L4	1 Gbps	2 Gbps	4 Gbps	10 Gbps	16 Gbps	24 Gbps
Dominios virtuales	10	20	20	40	60	80
Soporte de vCPU (máximo)	1	2	4	8	16	32
Soporte de memoria (máximo)	Sin límites					
Soporte de interfaz de red (máximo)	10	20	40	40	80	80
Soporte de almacenamiento (primario / máximo)	Incluido					
Rendimiento	Depende del hardware					
Gestión	HTTPS, SSH CLI, Consola directa DB9 CLI, SNMP					

* Los valores reales de rendimiento pueden variar en función del tráfico de red y de la configuración del sistema.
Los resultados de rendimiento se obtuvieron utilizando un dispositivo con una CPU Intel i5-3550 a 3,30 GHz ejecutando VMware ESXi 6.0.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

Información para pedidos

Producto	SKU	Descripción
FortiADC 220F	FAD-220F	FortiADC 220F, 4 puertos GE RJ45, 4 puertos GE SFP, 1 unidad de almacenamiento SSD de 120 GB.
FortiADC 320F	FAD-320F	FortiADC 320F, 4 puertos GbE GE, 4 puertos SFP GE, 2 puertos SFP+ 10 GE, 2 puertos de gestión GE, 1 unidad SSD de 120 GB almacenamiento.
FortiADC 420F	FAD-420F	FortiADC 420F, 4 puertos GE RJ45, 4 puertos GE SFP, 4 puertos 10 GE SFP+, 2 puertos de gestión, 1 unidad de almacenamiento SSD de 120 GB, aceleración SSL por hardware, fuente de alimentación redundante opcional.
FortiADC 1200F	FAD-1200F	FortiADC 1200F, 8 puertos 10 GE SFP+, 8 puertos GE SFP, 8 puertos GE RJ45, 2 puertos de gestión GE RJ45, 1 unidad SSD de 240 GB, fuentes de alimentación de CA dobles.
FortiADC 1200F-DC	FAD-1200F-DC	FortiADC 1200F, 8 puertos 10 GE SFP+, 8 puertos GE SFP, 8 puertos GE RJ45, 2 puertos de gestión GE RJ45, 1 unidad SSD de 240 GB, fuentes de alimentación de CC dobles.
FortiADC 2200F	FAD-2200F	FortiADC 2200F, 12 puertos SFP+ 10 GE, 8 puertos SFP GE, 2 puertos de gestión RJ45 GE, 1 unidad SSD de 240 GB, CA doble fuentes de alimentación.
FortiADC 2200F-DC	FAD-2200F-DC	FortiADC 2200F, 12 puertos SFP+ 10 GE, 8 puertos SFP GE, 2 puertos de gestión RJ45 GE, 1 unidad SSD de 240 GB, doble CC fuentes de alimentación.
FortiADC 4200F	FAD-4200F	FortiADC 4200F, 4 QSFP+ de 40 GbE, 8 SFP+ de 10 GbE, puerto de gestión RJ45 de 2 GbE, unidad SSD de 480 GB, CA doble fuentes de alimentación.
FortiADC 4200F-DC	FAD-4200F-DC	FortiADC 4200F, 4 QSFP+ de 40 GbE, 8 SFP+ de 10 GbE, puerto de gestión RJ45 de 2 GbE, unidad SSD de 480 GB, doble CC fuentes de alimentación.
FortiADC 5000F	FAD-5000F	FortiADC 5000F, 4 QSFP28 de 100 GE, 8 QSFP de 40 GE, 1 puerto de gestión RJ45 de GE, 1 unidad SSD de 1.74 TB, alimentación de CA doble fuentes fijas.
FortiADC-VM01	FAD-VM01	Dispositivo virtual de software FortiADC-VM. Admite hasta 1 núcleo vCPU.
FortiADC-VM02	FAD-VM02	Dispositivo virtual de software FortiADC-VM. Admite hasta 2 núcleos vCPU.
FortiADC-VM04	FAD-VM04	Dispositivo virtual de software FortiADC-VM. Admite hasta 4 núcleos vCPU.
FortiADC-VM08	FAD-VM08	Dispositivo virtual de software FortiADC-VM. Admite hasta 8 núcleos vCPU.
FortiADC-VM16	FAD-VM16	Dispositivo virtual de software FortiADC-VM. Admite hasta 16 núcleos vCPU.
FortiADC-VM32	FAD-VM32	Dispositivo virtual de software FortiADC-VM. Admite hasta 32 núcleos vCPU.
Gestor central 10	FAD-CM-BASE	Clase de licencia de FortiADC Central Manager, gestiona hasta 10 dispositivos FortiADC, VMware vSphere.
Gestor central ilimitado	FAD-CM-UL	Clase de licencia de FortiADC Central Manager, gestiona un número ilimitado de dispositivos FortiADC, VMware vSphere.
Accesorios opcionales	SKU	Descripción
Fuente de alimentación redundante FortiADC	SP-FAD400F-PS	Fuente de alimentación de CA para FAD-400F y FAD-420F; el cable de alimentación SP-FGPCOR-XX se vende por separado.
	SP-FAD-1200F-PS	Fuente de alimentación de CA para FAD-1200F, 2200F y 4200F; el cable de alimentación SP-FGPCOR-XX se vende por separado.
Módulo de ventilador 400F	SP-FAD400F-VENTILADOR	Módulo de ventilador para FAD-400F.
Módulo de ventilador 1200F/2200F	SP-FAD1200F-VENTILADOR	Módulo de ventilador para FAD 1200F y 1200F.
5000F SSD	SP-FAD5000F-SSD	SSD SATA de 1,84 TB y 2,5 pulgadas con bandeja para FAD-5000F.
Suscripciones VM	SKU	Descripción
Las suscripciones VM son compatibles con todas las VM desde VM01 (1 CPU) y hasta VM32 (32 CPU).		

* Todos los hardware de forma (suscripción BM/VM/VM) están disponibles con diferentes procesos de licencias, como seguridad de redes, seguridad de aplicaciones y seguridad de IA.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo R.D.

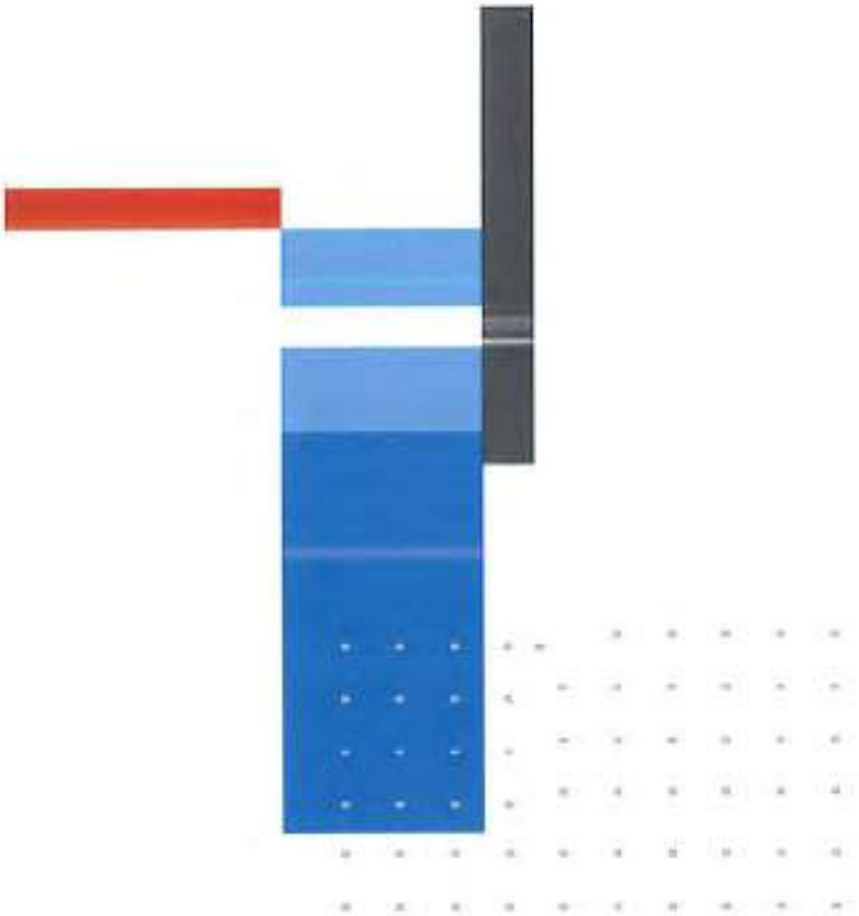
464-13

Política de responsabilidad social corporativa de Fortinet

Fortinet se compromete a impulsar el progreso y la sostenibilidad para todos a través de la ciberseguridad, respetando los derechos humanos y las prácticas empresariales éticas, haciendo posible un mundo digital en el que siempre se pueda confiar. Usted declara y garantiza a Fortinet que no utilizará los productos y servicios de Fortinet para participar en, o apoyar en alguno, violaciones o abusos de los derechos humanos, incluidos aquellos que impliquen censura ilegal, vigilancia, detención o uso excesivo de la fuerza. Los usuarios de los productos de Fortinet están obligados a

cumplir con el EULA de Fortinet de Fortinet.e informar de cualquier sospecha de violación del EULA a través de los procedimientos descritos en la política de privacidad

Política de denuncia de irregularidades.





FORTINET

Copyright © 2024 Fortinet, Inc. Todos los derechos reservados. Fortinet®, FortiGate®, FortiCare® y FortiGuard®, y algunas otras marcas son marcas registradas de Fortinet, Inc, y otros nombres de Fortinet en este documento pueden ser marcas registradas y/o marcas de derecho consuetudinario de Fortinet. Todos los demás nombres de productos o empresas pueden ser marcas comerciales de sus respectivos propietarios. El rendimiento y otras métricas aquí contenidas se obtuvieron en pruebas de laboratorio internas en condiciones ideales, y el rendimiento real y otros resultados pueden variar. Las variables de red, las distintas versiones de red y otras condiciones pueden afectar a los resultados de rendimiento. Nada de lo aquí contenido representa un compromiso vinculante por parte de Fortinet, y Fortinet renuncia a todas las garantías, ya sean expresas o implícitas, excepto en la medida en que Fortinet suscriba un contrato vinculante por escrito, firmado por el VP Legal de Fortinet y suscrito, con un comprador que garantice expresamente que el producto identificado funcionará de acuerdo con dichas métricas de rendimiento expresamente identificadas y, en tal caso, solo las métricas de rendimiento específicas expresamente identificadas en dicho contrato vinculante por escrito serán vinculantes para Fortinet. Para evitar cualquier duda, cualquier garantía estará limitada al rendimiento en las mismas condiciones ideales que en los ensayos de laboratorio internos de Fortinet. Fortinet renuncia por completo a cualquier acuerdo, declaración y garantía en virtud del presente, ya sea expresa o implícita. Fortinet se reserva el derecho a cambiar, modificar, transferir o revisar de cualquier otra modo esta publicación sin previo aviso, y se aplicará la versión más actualizada de la misma.

464-14

Mühlbauer
High Tech International

CLP 60

SISTEMA DE PERSONALIZACIÓN DE TARJETAS

El CLP 60 de Mühlbauer es un sistema de personalización de tarjetas de sobremesa de última generación. El rendimiento es de hasta 150 tarjetas por hora. Con más de 100 sistemas instalados y más de 20.000 documentos producidos, la serie CLP ha sido probada con éxito por los clientes. Este sistema es la mejor solución para la personalización descentralizada de identidad, permisos de conducir y otras tarjetas inteligentes basadas en el formato ID-1. Ofrece la misma calidad que los sistemas de gran volumen. Su pequeño tamaño, bajo peso y diseño compacto facilitan su manejo y transporte. La máquina tiene una interfaz de usuario intuitiva y puede manejarse mediante una pantalla táctil. Las tareas de personalización de la CLP son aptas para todas las tarjetas de contacto, sin contacto y de doble interfaz.



MÓDULOS CLAVE*

- Apilador de entrada de tarjetas
- Inspección visual
- Apilador de salida de tarjetas
- Codificación de chips (con contacto y/o sin contacto)
- Grabado por láser

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.



464-15

Mühlbauer
High Tech International

CLP 60

CARACTERÍSTICAS Y VENTAJAS

CARACTERÍSTICAS PRINCIPALES

- Sistema compacto de personalización de sobremesa de diseño industrial
- Adecuado para requisitos de personalización
- Ofrece la misma calidad de personalización que las máquinas de personalización Mühlbauer de volumen medio y alto
- Servicio directo y tiempo de reacción rápido (terceros proveedores de láser)
- Sistema de refrigeración silencioso optimizado
- Unidad de aspiración láser integrada con fibras de carbono activas
- MB MCES o MB MCES, incluido MB Product Designer
- Conexión de datos a la red y a otras bases de datos externas
- MB INCAPE & MB PalaMax* listo

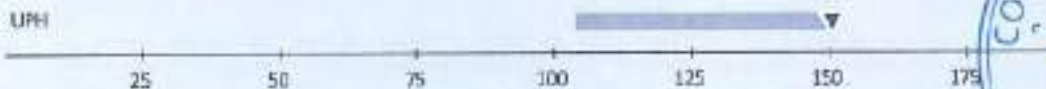
PRODUCTIVIDAD / UNIDADES DE PROCESO / CARACTERÍSTICAS

- Alimentación de tarjetas desde el apilador de entrada con gran autonomía de hasta 200 tarjetas
- Alimentador manual de tarjetas adicional para una producción rápida
- Entrada/salida bloqueable con ventana de visualización para controlar fácilmente el volumen de la tarjeta
- Codificación por chip con contacto / sin contacto / doble interfaz
- Sistema de grabado por láser con ventana de visualización
- Sistemas de control de visión con sistema de iluminación LED para ambas caras de la tarjeta
- Estación giratoria para grabado láser frontal y posterior incl. unidad giratoria en dirección y
- Unidad de giro de tarjetas en los ejes X e Y para aplicaciones láser de seguridad (CLI, MLI) y alineación láser
- Pantalla táctil en color con GUI de Mühlbauer
- Asas retráctiles para facilitar el desplazamiento/transporte del Sistema

* Más módulos de personalización como por ejemplo color pueden ser incorporados bajo solicitud y costos adicionales.

DATOS TÉCNICOS

- Tipos de tarjetas: formato / materiales: Tarjetas ID-1 / PC, PVC, ABS, PET, PETG, tarjetas metálicas; otras bajo pedido.
- Tipos de módulos IC: Módulos procesadores: T=0 / T=1
- Módulos de memoria: Bus I2C / 2;3 hilos
- Sin contacto: ISO 14443 / 15693
- Interfaz: Ethernet
- Rendimiento: hasta 150 tarjetas por hora; en función del proceso
- Opción de control de acceso del operador
- Función de alineación automática
- Garantiza un resultado de personalización láser constante en todos los equipos instalados
- Ideal para una solución descentralizada con calidad homogénea en todos los centros



CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

Grupo MÜHLBAUER

FICHA TÉCNICA

CLP 60

Solución para la personalización de tarjetas



CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

464-17

1. Puestos de trabajo disponibles

- CLP 60

2. Dimensiones

Módulo	mm			pulgada		
	Altura	Longitud	Profundidad	Altura	Longitud	Profundidad
CLP 60	591	598	548	23,27	23,54	21,58
Dimensiones totales	591	598	548	23,27	23,54	21,58

3. Peso

Módulo	en kg
CLP 60	75*
Mesa opcional	120
Peso total sin mesa	75*

- con MB Laser

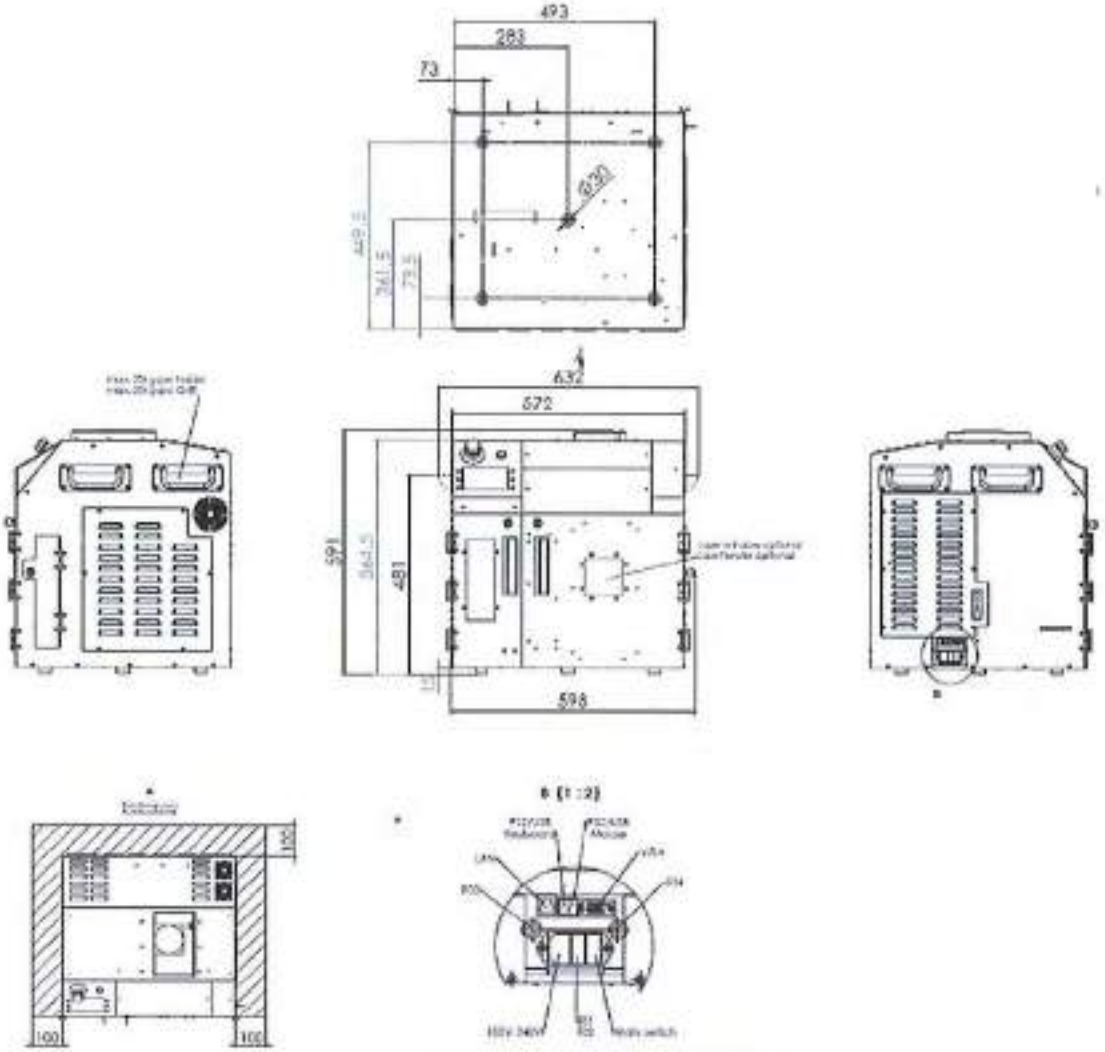
4. Instalaciones

Máquina eléctrica	Tensión:	110 V - 220 V	Potencia - Conexión:
	Tolerancia:	± 10 %	16 A Conector Schuko
	Protección:	10 A	
	Frecuencia:	50/ 60 Hz	
	Consumo:	Aprox. 0,66 kVA	
Ruido aéreo	Valor máximo del nivel de presión acústica de emisión		54,00 dB(A)
Entorno de producción	Requisitos	Temperatura:	23 °C± 3 °C
		Humedad:	50 %± 10 %

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

464-18

5. Plano de disposición de la máquina



do la sala: aprox. 1500 x 1500 x h 3000 mm

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

EMDOC
CONSORCIO

Carta de Presentación

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

EMDOC
CONSORCIO

25 de febrero de 2025

Señores
Junta Central Electoral
Santo Domingo, R. D.

Atención: **Comité de Compras y Contrataciones**

Referencia: **JCE-CCC-LPI-2024-0001**

Distinguidos señores:

Por este medio de la presente comunicación tenemos a bien presentar a nuestra asociación de empresas para el proceso de Licitación Pública Internacional de referencia, dando una breve descripción de nuestra experiencia y principales atributos:

Somos el **Consorcio EMDOC,** formado por las empresas siguientes:

- IQTEK SOLUTIONS S.R.L.
- MÜLHLBAUER ID SERVICES GMBH
- GSI INTERNATIONAL INC.
- ULTRA TECH INC. S.A.
- VERIDOS GMBH

El **Consorcio EMDOC** fue constituido el 27 de enero de 2025, en la ciudad de Santo Domingo, Distrito Nacional de la República Dominicana, con el objeto de preparar y presentar conjuntamente la oferta para la licitación pública e internacional No. **JCE-CCC-LPI-2024-0001** y, en caso de resultar adjudicatario de dichos trabajos, ejecutar el proyecto bajo la forma jurídica de asociación de empresas que se establezca conforme a las bases de dicha licitación y a la Legislación Dominicana.

Las empresas que forman parte del **Consorcio EMDOC** cuentan con profesionales con una amplia experiencia en el sector de las tecnologías de la información y en el diseño e implementación de proyectos seguros de identificación nacional, así como su mantenimiento, soporte y garantía. El **Consorcio EMDOC** busca ofrecer soluciones tecnológicas confiables, seguras y de alto rendimiento, con el más alto nivel de calidad para las empresas, para así satisfacer las necesidades de los clientes y cumplir sus metas.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

iQtek Mühlbauer GSI ULTRATECH VERIDOS
Ave. 27 de febrero esquina Ave. Tiradentes, Torre Friusa, Local B-B
Santo Domingo, Rep. Dominicana. Tel. (809) 412-9312

Contamos en nuestro haber con decenas de proyectos exitosos de identidad nacional similares o que exceden en su alcance al requerido en la presente licitación, como son:

- Cedula de Identidad Nacional con PKI en Ecuador
- Pasaporte Electrónico con PKI en Guyana Inglesa
- Licencia de conducir en Panamá y El Salvador
- Pasaporte electrónico con PKI en Costa Rica
- Registro vehicular y suministro de placas en El Salvador
- Tarjeta de circulación vehicular de Panamá
- Sistemas de datos biométricos en República Dominicana, Panamá, Costa Rica, El Salvador, Nicaragua, Uruguay y Ecuador

El **Consorcio EMDOC** será aliado estratégico para la JCE en el cumplimiento exitoso de cada de las etapas del contrato, en caso de ser adjudicado.

Atentamente,

Bernardo Pérez
Apoderado Legal
Consorcio EMDOC

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

iOtek Müllmann High Tech International GSI ULTRATECH VERIDOS
Ave. 27 de febrero esquina Ave. Tiradentes, Torre Frisa, Local 8-B
Santo Domingo, Rep. Dominicana. Tel. (809) 412-6312

EMDOC
CONSORCIO

4167-1

Visión del Proyecto

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

EMDOC
CONSORCIO

VISIÓN DEL PROYECTO

Nuestra Vision se centra en proveer un sistema seguro, eficiente y accesible que garantice la autenticidad y protección de la identidad de los ciudadanos. Nuestra solución para la impresión de la nueva cedula de identidad y electoral (CIE) y Cedula de Identidad (CI) estará alineado a estándares internacionales, el cual incluirá tecnologías avanzadas para ofrecer servicios de identificación modernos y confiables.

Nuestra solución incluye la impresión de ocho (8,000,000) millones de CIE y CI, durante los primeros dieciocho (18) meses de ejecución, garantizando el suministro oportuno y seguro de los equipos, materiales y servicios necesarios para el cumplimiento del Proceso de Licitación Pública Internacional JCE—CCC-LPI-2024-0001

Importante mencionar que nuestra solución propone incorporar nuevas tecnologías que aporten mayores niveles de seguridad, modernización y mejoras en los servicios que ofrece la Junta Central Electoral a la ciudadanía, relacionados con la función electoral y las atribuciones que la Carta Magna le otorga, en materia del Registro Civil y de la Cédula de Identidad.

La solución propuesta incluye.

1. **Seguridad y protección de datos:** Implementación de medidas robustas de seguridad que aseguren la integridad y confidencialidad de la información personal, previniendo fraudes y suplantaciones de identidad.

2. **Eficiencia en la emisión:** Optimizar los procesos para que la emisión y renovación de documentos de identidad sean rápidos y sencillos, reduciendo tiempos de espera y mejorando la experiencia del ciudadano.

3. **Accesibilidad geográfica:** Desplegar unidades móviles y puntos de actualización en diversas localidades, especialmente en zonas rurales, para garantizar que todos los ciudadanos tengan acceso equitativo a los servicios de identificación.

4. **Adopción de tecnologías avanzadas**: Incorporar soluciones como chips electrónicos, biometría facial y dactilar, y sistemas de autenticación digital, para fortalecer la seguridad y facilitar la integración con plataformas digitales.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

5. **Cumplimiento de estándares internacionales:** Asegurar que los documentos emitidos cumplan con normativas globales, permitiendo su reconocimiento y aceptación en otros países y facilitando la movilidad internacional de los ciudadanos.

Beneficios:

- **Reducción del fraude:** Al implementar tecnologías de seguridad avanzadas, se disminuye la posibilidad de falsificación y uso indebido de los documentos de identidad.

- **Mejora en la prestación de servicios públicos y privados:** Un sistema de identificación confiable facilita el acceso a diversos servicios, desde trámites gubernamentales hasta operaciones bancarias y comerciales.

- **Fomento de la inclusión digital:** Proveer a los ciudadanos de herramientas de identificación electrónica que promuevan su participación en la economía digital y en plataformas de gobierno electrónico.

- **Fortalecimiento de la confianza ciudadana:** Un sistema transparente y eficiente en la emisión de documentos de identidad Segura que refuerzan la confianza de la población en las instituciones gubernamentales

Como parte de los componentes que se incluyen como parte de la solución propuesta se incluyen:

1. Tarjetas CIE y CI
   - Plásticos electrónicos en policarbonato
2. Máquinas de Impresión
3. Cédula Digital (en el celular). Se refiere a un sistema de emisión de cédulas digitales. El oferente tiene que cotizar un sistema de emisión de cédula digital como máximo un 10% de la producción física de tarjetas al año.
4. PKI con establecimiento de Autoridad de Certificación
5. Kits periféricos
   - Escáner
   - Lector de firma
   - Lector de huellas
   - Impresora térmica de punto de venta
   - Lector de huellas digital persona
   - Cámara
   - Lector RFID
6. Servicio de Instalación y Mantenimiento
7. Capacitación

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo

EMDOC
CONSORCIO

Curriculum del líder del proyecto o jefe de proyecto

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo

JOSE DAVID VARGAS BUSTAMANTE

471

Administrador De Proyectos Senior, MPM, PMP, PMO, SMC

Resumen de principal experiencia

GSI INTERNATIONAL INC. — **San José, Costa Rica**
Administrador de proyectos senior — *2012 - Presente*

Responsable de la gestión de los proyectos desde su origen hasta su implementación final, trabajando de la mano con clientes externos y diferentes equipos de implementación. Entre mis responsabilidades se encuentran:

- Lidero diferentes tipos de proyectos clave bajo metodologías iterativas y ágiles
- Defino el alcance del proyecto y sus objetivos
- Planifico, monitoreo y controlo, múltiples proyectos y equipos
- Garantizar una comunicación rápida entre las partes interesadas y la alta calidad en las entregas a tiempo
- Gestiono la calidad, recursos, presupuestos, calendarios y otros
- Identifico y desarrollo nuevas oportunidades con los clientes y los equipos de preventa

Los principales proyectos que dirijo se centran en el desarrollo de software a la medida, automatización de procesos con BPM y proyectos de gestión de contenido.

Infosgroup — **San José, Costa Rica**
Gerente de cuentas estratégicas y proyectos — *2006 -2012*

Gestioné las cuentas estratégicas (clientes locales y regionales) en donde en conjunto con el personal de negocio identifiqué, desarrollé y gestioné oportunidades de proyectos desde su conceptualización hasta su implementación.

- Responsable de la búsqueda de oportunidades del negocio y la innovación de soluciones, que puede resultar en beneficios y mejoras para los clientes
- Comprender y gestionar las necesidades de los clientes y transformarlos en iniciativas reales y proyectos exitosos
- Definición y gestión del alcance del proyecto, requerimientos, presupuesto, cronogramas, riesgos y ejecutar los proyectos bajo metodologías iterativas y el PMBOK.
- Gestión de proyectos bajo metodologías como (RUP, SCRUM, PMBOK) desde la conceptualización del proyecto hasta su implementación.
- Analista de negocio/Dueño del Producto como interlocutor entre el negocio y los equipos de desarrollo
- Miembro de equipo seleccionado para definir e implementar nuevos procesos de Desarrollo de Software y Gestión de Proyectos para lograr la certificación en el CMMI nivel 3. Logramos la certificación siendo la primera compañía en América Latina en obtener dicha acreditación.

Los proyectos dirigidos se centraron en el desarrollo de software a la medida, portales web (CMS), automatización de procesos con BPM, proyectos de integración y creación de servicios, pruebas y otros servicios de consultoría especializados.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

Educación

Universidad para la Cooperación Internacional, 2012
(stría en Administración de Proyectos

Universidad Cenfotec, 2002
Especialista en Desarrollo de Software

Universidad Latinoamericana de Ciencia y Tecnología, 2002
Licenciatura en Administración de Negocios con énfasis en Banca y Finanzas

Universidad Latinoamericana de Ciencia y Tecnología, 1999
Bachiller en Administración de Negocios con énfasis en Banca y Finanzas

Certificaciones

PMO Global Alliance	Project Management Office Certified Practitioner (PMO)	2018	Certificate Number CP-0692
Scrum Alliance	Scrum Master Certified (SMC) Scrum Funcamentals	2017 2017	Certificate ID 595215
Project Management Institute	Project Management Professional (PMP)	2016	PMP Number 1940485
Rational University	Certificación en fundamentos del Rational Unified Process (RUP) Certificación en Administración de Requerimientos	2003 2003	

CONSORCIO EMDOC
EMDOC CONSORCIO
Santo Domingo

PUNTO 3.1.6 DOCUMENTOS TECNICOS

3.1.6.1 Resumen ejecutivo

DAVID VARGAS – c) LIDER DEL PROYECTO

Experiencia de 5 años en uno o varios proyectos de identificación de tarjetas policarbonatos	Certificación de PMP	Conocimientos ITIL
PROYECTO DE PASAPORTE BIOMETRICO ELECTRONICO DE POLICARBONATO Año 2019 Republica de Costa Rica [redacted] Descripción del proyecto: El Fideicomiso Fondo Especial de Migración JADGME – BCR adquirió mediante el proceso de licitación "2019PP-000068-0018200001" el Pasaporte Biométrico" la adquisición de un sistema de emisión de pasaportes, compra de equipo tecnológico, impresora para la impresión de libretas electrónicas de pasaportes, Libretas electrónicas de pasaporte y soporte y mantenimiento a la empresa GSI INTERNATIONAL INC. Contrato por un valor aproximado de 39 millones de USD a la fecha. La contratación incluyó el desarrollo, instalación, configuración, capacitación, entrega y servicio de soporte y mantenimiento de los siguientes componentes: Pasaportes de Emergencia, para personas naconsles de la República de Costa Rica Documentos de Identidad de Viaje para personas extranjeras. Documentos de Viaje Biométricos (electrónicos), para personas refugiadas, apátridas y asiladas políticas (hoja de datos de policarbonato y foto a color) Pasaportes Ordinarios Biométricos (electrónicos), para personas nacionales de la República de Costa Rica (hoja de datos de policarbonato y foto a color) Desarrollo del sistema de gestión y emisión de documentos migratorios, con sus interfaces (web services) y capacitación del sistema Solución integral (hardware y software) PKI Solución de Impresión de Documentos Migratorios, para Pasaportes Biométricos y Documentos de Viaje (policarbonato con chip y foto a color, impresoras láser full in line) 100 cámaras Faciales digitales Canon 100 escáneres de Huellas Digitales 4-4-2 80 dispositivos de Captura de Firmas 15 maletas móviles de enrolamiento biométrico 100 estaciones de trabajo (CPU, Monitor, Teclado, Mouse)	Se incluye certificado PMP vigente hasta 2025	Se incluye certificado de Fundamentos de ITIL: La mejora de Servicios

CONSORCIO EMDOC
EMDOC CONSORCIO
Santo Domingo, R.D.

100 scanner de documentos Fujitsu 50 lectores de una sola Huellas 100 lectores de pasaportes con OCR y lector de chip, para realizar el control de calidad y entrega de los documentos migratorios. Más de 600,000 libretas de pasaportes electrónicos con página de policarbonato han sido entregadas a la fecha. Soporte y Mantenimiento a toda la solución provista. Licenciamiento Ilimitado de E-power y Quick-scan		
FABRICA DE DOCUMENTO DE IDENTIDAD PERSONAL (Cedula) +SISTEMA BIOMETRICO DE IDENTIFICACION CIUDADANA (ABIS): Año 2016 hasta año 2022 República de Panamá: **Descripción del proyecto** Solución de impresión para el documento de identidad personal panameño (Cedula). Contrato N0.24/2016/DS Provisión, Desarrollo de Sistemas tales como Sistema de Gestor de Hardware, gestor de producción, gestor de Inventarios, distribución, reportes, entre otros (Impresora de documento de identidad personal) y Suministros de 4,500,000 tarjetas (Documento de Identidad Personal) equipamiento tecnológico, aplicativo, Insumos y servicio de mantenimiento y soporte para el centro de impresión de documento de identidad personal del Tribunal Electoral de Panamá Valor aproximado del contrato $.6,519,565.42 seis millones quinientos diecinueve mil, quinientos sesenta y cinco con 42/100 dólares de los Estados Unidos de América. ABIS: Numero de registros soportado el sistema ABIS El volumen es de (10,000,000) diez millones de registros (personas) Suministro, instalación y soporte, mantenimiento y actualización del sistema biométrico de identificación ciudadana (ABIS), para la extracción, conversión y migración de todos los datos del sistema actual a la nueva solución para ser utilizada en la Dirección de Tecnología de la Información y comunicación (DTIC) del Tribunal Electoral de Panamá. Contrato de soporte y mantenimiento para el sistema Impresión/emisión.		

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo

THIS IS TO CERTIFY THAT

Jose David Vargas Bustamante

HAS BEEN FORMALLY EVALUATED FOR DEMONSTRATED EXPERIENCE, KNOWLEDGE AND PERFORMANCE IN ACHIEVING AN ORGANIZATIONAL OBJECTIVE THROUGH DEFINING AND OVERSEEING PROJECTS AND RESOURCES AND IS HEREBY BESTOWED THE GLOBAL CREDENTIAL

Project Management Professional (PMP)®

IN TESTIMONY WHEREOF, WE HAVE SUBSCRIBED OUR SIGNATURES UNDER THE SEAL OF THE INSTITUTE

Jennifer Tharp
Chair, Board of Directors

Mike DePrisco
Interim President & CEO

PMP® Number: 1940485
PMP® Original Grant Date: 07 July 2016
PMP® Expiration Date: 06 July 2025

Project Management Institute.

LinkedIn Learning

Fundamentos de ITIL: La mejora de servicios

Curso completado por José David Vargas B, PMP, PMO-CP, CSM, LSSGBPC
may 29, 2024 at 12:08a. m. UTC • 42 minutos

Aptitudes que se tratan

ITIL

CONSORCIO EMDOC, Santo Domingo, RD

Responsable de estrategia de contenido de Learning

ID del certificado: c9414aa070835411cac54aaa49d0b7c7644641923e7ef9309d3cc1001c7818

PMO GLOBAL ALLIANCE

PMO-CP

PMO CERTIFIED PRACTITIONER

THIS IS TO CERTIFY THAT

José David Vargas Bustamante

HAS SUCCESSFULLY COMPLETED THE REQUIREMENTS TO BE RECOGNIZED BY PMO GLOBAL ALLIANCE AS A

PMO CERTIFIED PRACTITIONER (PMO-CP®)

AMERICO PINTO
CHAIR, PMO GLOBAL ALLIANCE

CANDIDATE NUMBER: 3824941

CERTIFICATE NUMBER: 13702072

EFFECTIVE FROM: September 6, 2019

NO EXPIRATION DATE

PMO GLOBAL ALLIANCE

478

El suscrito, Juan Chow Wong, Notario Público con oficina en San José, calle cinco, entre avenidas central y primera, frente antiguo Cine Variedades, segundo piso de Edificio Montealegre Quijano, certifica: Que el anverso de las anteriores tres fotocopias, numeradas del uno al tres, selladas y firmadas en la parte superior derecha, son reproducciones fieles y exactas de sus originales, las cuales he tenido a la vista, y corresponden a Certificados de participación extendidos a nombre de José David Vargas Bustamante. Certifico de conformidad con el artículo ciento diez del Código Notarial, a solicitud de la sociedad Grupo de Soluciones Informáticas GSI, S.A., cédula jurídica número tres-ciento uno-cero setenta y tres mil ochocientos noventa y tres, en San José, a las ocho horas del treinta y uno de mayo del año dos mil veinticuatro. La presente certificación corresponde al número ochenta y cuatro-veinticuatro, del consecutivo que al efecto lleva el suscrito Notario. El presente documento es para ser utilizado en República Dominicana. Agrego y cancelo los timbres de ley. Juan Chow.

LIC. JUAN CHOW WONG
NOTARIO PÚBLICO
C. 8511

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

479

Banco de Costa Rica
Oficina:937 BARRIO AMON
Fecha:22/04/2024 Hora:10:38:54

Detalle de Tasacion
Tasacion:524862648 Entero:554196115

Pagado

TIMBRE FISCAL	15.00

22 ABR 2024

CAJERO AUXILIAR

Moneda de Transaccion:	COLONES
Sub Tot. Timbres:	15.00
Descuento:	0.90
Total Timbres:	14.10

Banco de Costa Rica
Oficina:937 BARRIO AMON
Fecha:22/04/2024 Hora:10:40:52

Detalle de Tasacion
Tasacion:524863180 Entero:554196921

Pagado

TIMBRE FISCAL	125.00
TIMBRE COLEGIO DE ABOGADO	275.00

22 ABR 2024

Moneda de Transaccion:	COLONES
Sub Tot. Timbres:	400.00
Descuento:	24.00
Total Timbres:	376.00

Banco de Costa Rica
Oficina:937 BARRIO AMON
Fecha:22/11/2023 Hora:10:04:28

Detalle de Tasacion
Tasacion:509972870 Entero:531829731

Pagado

TIMBRE FISCAL	15.00
TIMBRE ARCHIVO NACIONAL	5.00

22 NOV 2023

Moneda de Transaccion:	COLONES
Sub Tot. Timbres:	20.00
Descuento:	1.20
Total Timbres:	18.80

Banco de Costa Rica
Oficina:937 BARRIO AMON
Fecha:24/04/2024 Hora:11:15:39

Detalle de Tasacion
Tasacion:525179577 Entero:554673240

Pagado

TIMBRE PARQUES NACIONALES	500.00
TIMBRE FISCAL	125.00

OFICINA BARRIO AMON

24 ABR 2024

Moneda de Transaccion:	COLONES
Sub Tot. Timbres:	625.00
Descuento:	37.50
Total Timbres:	587.50

NICOLE SOLIS ROMERO
CAJERA

480

DIRECCIÓN NACIONAL DE NOTARIADO | GOBIERNO DE COSTA RICA

DIRECCIÓN NACIONAL DE NOTARIADO
REGISTRO NACIONAL DE

AUTENTICACIÓN 347212-2024

TRÁMITE: 200014

LICDA. MARÍA PAULA AGÜERO BENAMBURG, FUNCIONARIA AUTORIZADA DE LA DIRECCIÓN NACIONAL DE NOTARIADO DE LA REPÚBLICA DE COSTA RICA; HACE CONSTAR: Que la FIRMA del Notario Público JUAN CHOW WONG, CÉDULA 800750027, CARNÉ NÚMERO 8511, es similar a la que se encuentra registrada en el Registro Nacional de Notarios de esta Dirección. Que a la fecha en que el Notario expidió el documento adjunto, se encontraba habilitado para el ejercicio del notariado. ADVERTENCIAS DE NULIDAD Y VALIDEZ: Si este folio es desprendido de los folios adjuntos, o los sellos de esta Dirección que sirven de liga o unión con dicho folio se encuentran "rotos" o alterados, la razón de autenticación queda automáticamente anulada. El presente trámite de legalización de firma no implica convalidación,ni prejuzga sobre la legalidad, validez, eficacia, autenticidad o legitimidad del documento adjunto ni de su contenido, así como tampoco de la solvencia tributaria relacionada directa o indirectamente con dicho documento, por consiguiente tampoco implica aval ni responsabilidad alguna de la Dirección Nacional de Notariado ni del funcionario que la expide, todo lo cual es responsabilidad exclusiva del fedatario; Asimismo, no enerva las acciones administrativas y disciplinarias que contra el Notario correspondan, derivadas de irregularidades notariales advertidas o que se llegaran a advertir con posterioridad. -ES CONFORME.- San Pedro de Montes de Oca, a las nueve horas cincuenta y uno minutos del cuatro de junio del dos mil veinticuatro. Se agregan y cancelan los timbres de ley. (ÚLTIMA LÍNEA)

Licda. María Paula Agüero Benamburg
Funcionaria Autorizada
Res. No. DNN-DE-051-2020

421

REPÚBLICA DE COSTA RICA

MINISTERIO DE RELACIONES EXTERIORES Y CULTO

A-1106212

APOSTILLE

(Convention de La Haye du 5 octobre 1961)

1. País: Costa Rica
(Country – País:)

Código: MCDWT2FTAMR
(Code – Code:)

El presente documento público
(This public document – Le présent acte public)

2. Ha sido firmado por: María Paula Agüero Benamburg
(Has been signed by – A été signé par:)

3. Actuando en calidad de: Certificador de Registro
(Acting in the capacity of – Agissant en qualité de:)

4. Lleva el sello/estampilla de: Dirección Nacional de Notariado
(Bears the seal/stamp of – Est revêtu du sceau/timbre de:)

Certificado
(Certified – Attesté)

5. En: San José, Costa Rica
(At – A:)

6. El: 06/06/2024
(On – Le:)

7. Por: Ivannia Espinoza Rodríguez , Oficial de Autenticaciones
(By – Par:) Ministry of Foreign Affairs – Ministère des Affaires Étrangères

8. No.: 1101285
(Under number – Sous le numéro:)

9. Sello:
(Seal – Sceau:)

10. Firma:
(Signature – Signature:)

1106212

Esta apostilla / legalización sólo certifica la autenticidad de la firma, la capacidad del signatario y el sello o timbre que ostenta. Ésta no certifica el contenido del documento para el cual se expidió.

This apostille / legalization only certifies the signature, the capacity of the signer and the seal or stamp it bears. It does not certify the content of the document for which it was issued.

Cette apostille / legalization ne certifie que la signature, la qualité en laquelle le signataire de l'acte a agi, et le sceau ou timbre dont cet acte est revêtu. Elle ne certifie pas le contenu du document pour lequel elle a été émise.

La autenticidad de esta apostilla / legalización puede ser verificada en: - The authenticity of this apostille / legalization may be verified at: - L'authenticité de cette apostille / legalization peut être vérifiée sur: http://www.rree.go.cr

EN BLANCO
-SIN TEXTO-
DNN Dirección Nacional de Notariado

CONSORCIO EMDOC
EMDOC
Santo Domingo, R.D.

Curriculum del personal técnico certificado en tecnología de impresión de tarjetas de identidad

CONSORCIO EMDOC
EMDOC CONSORCIO
Santo Domingo, RD

YORLIN YASSIEL REYES MIRANDA
yorlinreyes@yahoo.com
Panamá
Ciudad de Panamá
Tel.(507)229-6486/(507)6957-3295

EDUCACION

2004-2005 **INCAE** **MANAGUA, NICARAGUA**
Maestría de Administración Empresas

2002-2003 **UNIVERSIDAD TECNOLÓGICA DE PANAMÁ**
PANAMÁ, PANAMÁ
Post-Grado en Alta Gerencia

1995-2001 **UNIVERSIDAD SANTA MARÍA LA ANTIGUA (USMA)**
PANAMÁ, PANAMÁ
Licenciatura en Ingeniería Electrónica. Énfasis en comunicaciones

EXPERIENCIA

Mar-08 a Actual **GSI INTERNATIONAL INC.**
PANAMÁ, PANAMÁ
(Gerente de Operaciones)

- Dirijo, superviso y evalúo la operación de aproximadamente noventa (90) colaboradores en diez (10) sucursales ubicadas a lo largo de todo el país.
- Superviso y reviso los controles en las sucursales de productos entregados versus los insumos utilizados de sucursales
- Brindo seguimiento a las oportunidades del sistema y de esta manera lograr para el buen funcionamiento de la operación y así, desarrollar un producto de acuerdo a los estándares de nuestro cliente.
- Reviso, y superviso los procesos para reducir los tiempos de atención.
- Reviso y superviso los procesos para desarrollar las mejoras de las aplicaciones y así, se reduzcan los errores de los operadores.
- Realizo reportes semanales para la Junta Directiva de la Empresa relacionados con la operación.
- Experto en la calidad de los Documentos de Identidad Personal de policarbonto y pasaporte electrónico (Cedula) para Ecuador y Panama.

Mar – 06 a Mar-08 **DOLLAR RENT A CAR**
PANAMÁ, PANAMÁ
(Gerente de Operaciones)
Franquicia de Alquiler de Autos

- Seguí los procedimientos y requisitos de la Franquicia con sede en Oklahoma, Estados Unidos.
- Supervisé y evalué aproximadamente treinta (30) personas en cuatro (4) sucursales en el país. Supervisé los controles de gasolina, autos de la flota e inventario de piezas de mantenimiento y de mecánica.
- Reduje el porcentaje de autos pendientes de mantenimiento en un 90%, y establecí controles para reducir los atrasos.
- Supervisé, coordiné y controlé el tiempo de respuesta de los talleres externos de hojalatería, mantenimiento, garantía y respuesta de trabajos de mecánica de los talleres externos.
- Implementé procedimientos de taller para la flota de alquiler y para los autos de ventas.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

3.1.6 Documentos Técnicos

3.1.6.1 Resumen ejecutivo

EXPERTO TECNICO CERTIFICADO EN TECNOLOGIA DE IMPRESIÓN DE TARJETAS DE IDENTIDAD

YORLIN YASSIEL REYES MIRANDA

TECNICO CERTIFICADO EN TECNOLOGIA DE IMPRESIÓN DE TARJETAS DE IDENTIDAD	CERTIFICACION	Detalle de la experiencia
Supervisión de la calidad de la impresión en todos los centros de impresión de cedulas	Se incluye el certificado de Muhlbauer	**Dirección General de Registro Civil, Identificación y Cedulación** **Republica de Ecuador**  Técnico responsable de la calidad de impresión de las tarjetas de identidad personal (Cedula). Experto en la calidad de los Documentos de Identidad Personal (Cedula) Dirección General de Registro Civil, Identificación y Cedulación Descripción de la contratación: Adquisición, implementación de un sistema informático para la emisión de documentos de identidad y pasaportes electrónicos y provisión de equipos, suscripciones – licencias de software, insumos y servicios conexos para la Dirección General de Registro Civil, Identificación y cedulación (DIGERCIC). Sistema para la emisión de documentos de Identidad personal (cedula) de policarbonato y pasaportes electrónicos, HSM, National PKD/ICAO PKD, ABIS Vigencia: Fecha 2019 a la fecha Infraestructura de centro de datos principal y secundario, equipamiento para agencias de atención a nivel nacional y en consulados de

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo

		Ecuador, para un total de 183 agencias de atención nacional para DIGERCIC y 25 agencias de Ministerio de Relaciones Exteriores y Movilidad Humana (MREMH). Este proyecto no incluyo los insumos de libretas de pasaportes. No incluyo el material para el Documento de identidad personal. Descripción detallada del proyecto: Suministro, instalación y configuración de un sistema Web descentralizado para el enrolamiento Personalización y emisión de documentos de identidad Personal en Policarbonato (100%) formato ID1 y pasaportes electrónicos (EPass) formato ID3 Sistema de inspección biométrico automatizado de huellas y rostro (ABIS) para 16 millones de registros. Sistema de servicios web para búsqueda 1 a 1 y 1 a N de huellas y rostros integrado al ABIS. Capacidad mínima de 10 mil a 20 mil búsquedas diarias Infraestructura de llave pública (PKI) y su integración y conexión al Directorio de claves públicas de la OACI, se incluyeron módulos de seguridad (HSM) para el resguardo de llaves. Suministro de infraestructura (hw), licencias, suscripciones de software necesarias para la implementación de un centro de datos primario en alta disponibilidad y un sitio secundario para la recuperación de desastres. Suministro de kits (equipos de captura biométrica, producción y entrega de documentos, ambos en esquema descentralizado. Se incluyo como parte del proyecto la capacitación, transferencia de conocimientos, instalación, configuración, puesta en operación,

CONSORCIO EMDOC
EMDOC
CONSORCIO

		pruebas unitarias y de integración de los sistemas centrales. Migracion de la base de datos biométrica de más de 13.9 millones de registro. Este contrato incluyo el enrolamiento, personalización y emisión de pasaportes electrónicos en 25 agencias nacionales en Ecuador y 3 externas (Consulado de New York, Madrid y una oficina en Quito). Este contrato también incluyo la emisión en el Ecuador de cedulas de identidad personal en policarbonato en 183 agencias de acuerdo con los lineamientos de la OACI 9303. De igual forma incluyo servicios de post implementación, los cuales abarcan soporte técnico, mantenimiento preventivo y correctivo con niveles de servicio de 24x7x365 para todos los componentes del sistema. Importante señalar que como parte de un contrato complementario se contrató una solución de identidad digital y firma electrónica para la ciudadanía.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

487

Mühlbauer
High Tech International

CERTIFICATE

Yorlin Yassiel Reyes Miranda

employee of

GSI INTERNATIONAL, INC

has successfully attended a

SCP 801 Operation & Maintenance Training

at

03-05, 2022
40 HOURS

Mühlbauer
High Tech International

93426 Roding Germany
Phone: +49 9461 952-0
Fax: +49 9461 952-1101
Email: info@muhlbauer.de
Internet: www.muhlbauer.de

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

HOJA DE VIDA - PAULA HELENA CASTILLO RODRIGUEZ

EXPERIENCIA PROFESIONAL

GSI INTERNATIONAL INC.

Cargo: TECNICO CERTIFICADO EN TECNOLOGIA DE IMPRESIÓN DE TARJETAS DE IDENTIDAD - De abril 2016 a la fecha.

Como empleado de GSI INTERNATIONAL INC. participa en los procesos de diseño e implementación de Sistemas de gestión documental y archivos, implementación de aplicaciones de tecnología informática y en general la instalación. Participar en el proceso de capacitación a usuarios de los productos y sistemas implementados, Coordinación de proyectos, preparación de informes de avances y resultados de proyectos. Servicio de digitalización de documentos. Instalación y configuración de equipos informáticos.

Tipos de Proyectos en los que he participado:

- Panamá: Firma digital, seguridad en la impresión de documentos de identidad personal, Implementación en Sistema de Desarrollo a la medida, Conversión de rollos de microfilm a Digital, Digitalización de Documentos con firma electrónica, Proyecto archivística de expediente único Implementación de Sistema Biométrico, Piloto de Cédula Inteligente, Implementación del nuevo Sistema de Trámite en línea de Emisión de Licencias de Conducir, Migración de Datos.

- Regional: Implementación de Documentos Seguros como Pasaporte y Cédula de Ecuador, Implementación del Sistema de Validación Biométrica de puestos Fronterizo en Nicaragua.

Algunos de los clientes: GSI INTERNATIONAL INC. Panamá, Tribunal Electoral de Panamá, ENSA Panamá, Órgano Judicial, Registro Público, Ministerio de Economía y Finanzas, Centro Ann Sullyvan, St George Bank, Banco Aliado, DIGERCIC Ecuador, MIGOB Nicaragua, MOP, IMELCF, BDA, IFARHU, Dirección General de Ingresos de Panamá, entre otros.

Outsourcing - INFOSGROUP, S.A. PANAMÁ

Cargo: PROGRAM MANAGER

04 de enero 2016 al 26 de junio del 2016.

Rol: Gerencia del Proyecto Diseño e Implementación de un Sistema Informático de Administración de Recursos Humanos del Tribunal Administrativo Tributario (TAT).

Gestionar, Administrar y coordinar el equipo asignado y la coordinación previa con otros compañeros para la utilización de los recursos compartidos, para el cumplimiento de los hitos acordado con el cliente, esta solución de HCM y Payroll está basada en un aplicativo nativo de la empresa bajo el licenciamiento y herramienta Oracle.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

INFOSGROUP, S. A. PANAMÁ

Cargo: PROGRAM MANAGER, 18 de agosto 2014 – 15 de mayo del 2015.

Rol: Gerencia de Proyectos y Encargado del departamento de Servicios IT

- Administración de las actividades del Proyecto
- Gestión de Personal
- Gestión de riesgos y mitigación
- Control de calidad del proyecto
- Gestión con el cliente
- Gestión con Proveedores Locales
- Coordinación de los entrenamientos con el cliente
- Coordinación de las pruebas con el cliente
- Entregables y finalización del proyecto

Gestionar, Administrar y coordinar el equipo asignado y la coordinación previa con otros compañeros para la utilización de los recursos compartidos, para el cumplimiento de los hitos acordado con el cliente, esta solución de HCM y Payroll está basada en un aplicativo nativo de la empresa bajo el licenciamiento de Oracle.

Algunos de los clientes y proyectos donde he participado: Panamá Port, Indra Panamá, Colon Container, Zona Libre de Colón, Ensa, GDF Suez, Grupo MEC, Gran Terminal de Albrook, Telered.

GSI INTERNATIONAL INC.

Cargo: COORDINADOR DE PROYECTOS DEL AREA DE SOLUCIONES

01 marzo 2012 – 15 agosto 2014.

Rol: Gerencia de Proyectos

- Administración de las actividades del Proyecto
- Gestión de Personal
- Gestión de riesgos y mitigación
- Control de calidad del proyecto
- Gestión con el cliente
- Gestión con Proveedores Nacional e Internacionales.
- Administración de todas las empresas participantes dentro del proyecto
- Coordinación de los entrenamientos con el cliente
- Coordinación de las pruebas con el cliente
- Entregables y finalización del proyecto

He participado en proyecto con presupuesto de más de un millón de dólares, Programas de proyectos con 5 sub-proyectos.

Proyectos en lo que he participado: ATTT: Mejoramientos de la plataforma tecnológica fase I y II; Tribunal de Cuentas: Mejoramiento del Proceso de trámites de casos y digitalización de los expedientes; PanamaTech, Capital Bank, Benedetti & Benedetti, ANCORCO: instalación del Sistema de Gestión Documental, digitalización de documentos, Caja de Ahorros: nuevo portal web utilizando la plataforma de SharePoint 2010.



GOBIT SOLUTION

Cargo: CONSULTOR, 01 septiembre 2011 – 09 diciembre 2011.

Rol: Gerencia de Proyecto

- Realizar el Levantamiento de Proceso de Documentos para la aprobación de los Anteproyectos y Proyectos de Ley.
- Gestión de Personal y recursos
- Coordinación y ejecución de las entrevistas con los involucrados en el proyecto.
- Estimar los tiempos para la ejecución de los tiempos del proyecto.
- Entregables y finalización del proyecto.

Entrevistar, analizar y documentar los procesos de gestión documental para la aprobación de los proyectos de Ley en la Asamblea Nacional.

Cliente: Asamblea Nacional de Panamá.

INFOSGROUP, S.A. PANAMÁ

Cargo: CONSULTORA, 02 febrero de 2006 – 31 julio 2011.

Rol: Coordinador de Servicios IT/ Soporte y SaaS

- Administración de las aéreas de servicio (Soporte y SaaS)
- Gestión de Personal
- Atención a todos los clientes (soporte y SaaS)
- Mejora los procesos internos de ambos departamentos
- Diagnóstico de los procesos actuales para la implementación de la Norma EIC/ISO20000 e implementación de los estándares de ITIL V3.0
- Atención de los clientes a los cuales se les ofrece los servicios de Outsourcing de planilla.
- Métricas de los servicios IT
- Seguimiento a los proyectos de mejora en las aplicaciones de InfosWeb de planilla y ERP
- Negociación con los clientes internos y externos a nivel Gerencial
- Planificación y mitigación de riesgos

Rol: Coordinadora de Oficinas de Proyectos y ManPower (InfosPeople)

- Gestión de Proyectos con presupuesto de 250K
- Negociación a nivel Gerencial
- Gestión de Personal
- Coordinación y ejecución de Facturación de Proyecto
- Seguimiento y control de proyectos
- Participación en grupo de evaluación para la certificación CMMi Nivel 2
- Participación en grupo de evaluación para la certificación CMMi Nivel 3
- Ventas cruzadas de los servicios brindados por la empresa
- Métricas de rentabilidad de los proyectos

Implementación proyectos con presupuesto de más de un millón de dólares el cual se ejecutó como un programa de proyecto divido en 5 sub-proyectos.

Administración de Recursos y tareas con proveedores Internacionales y locales.

Proyectos en los que he participados: ATTT (Mejoramiento de la Plataforma Tecnológica Fase I y Fase II), Tribunal de Cuentas (Mejoramiento del proceso de trámites de casos y digitalización de expedientes), Panamá Tech (Digitalización de Expedientes), Benedetti & Benedetti, ANORCO (Instalación del Sistema de Gestión Documental y Digitalización de Expedientes), Caja de Ahorros (Nuevo Portal Web utilizando la plataforma de SharePoint 2010).

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

Rol: Documentadora

Proyecto COPA

- Confección de Manuales Técnicos
- Confección de Manuales de Instalación
- Confección de Manuales de Usuario
- Instalación de Sistemas
- Pruebas de las aplicaciones nuevas Aplicaciones
- Entrenamiento a personal sobre nuevas aplicaciones

SECRETARÍA DE LA PRESIDENCIA PARA LA INNOVACIÓN GUBERNAMENTAL, PANAMÁ

ASISTENTE TÉCNICO, septiembre 2003 a diciembre 2005.

- Evaluación de Proyectos para la adquisición de equipos en las Instituciones Gubernamentales.
- Auditoria de Sistemas implementados en las instituciones
- Diseño y Desarrollo de páginas Web.
- Encargada de comprar para la SI.
- Inventario del Proyecto Programa de Innovación y Proyecto Conéctate.
- Asistencia técnica a los usuarios

FORMACIÓN ACADÉMICA

2005 UNIVERSIDAD LATINA DE PANAMÁ, Licenciatura en Ingeniería de Sistemas Informáticos.

CERTIFICACIONES

- Sistema Administrador de Imágenes y Contenido ePower, Ver 4.5, Enero 2020.
- Sistema SmartCapture, Módulo de Captura Masiva de Documentos, Enero 2020
- eCapture – Módulo de Captura Masiva de Documentos, Panamá, Septiembre 2014
- 2021 – CretiProf, SCRUM Master Professional Certificate (SMPC) – Actualización
- 2020 – CertiProf, SCRUM Master Professional Certificate (SMPC)
- 2020 – AXELOS, ITIL Foundation Certificate in IT Services Management
- 2020 - CertiProf, SCRUM Foundation Professional Certificate (SFPC)
- 2016 – BS GROUP, Gestión de Riesgos en Proyectos (12 Professional Development Units recnocidas por el PMI – BSG-A 114).
- 2018 – Gestión Lean y Ágil de Proyectos. ID 21007
- 2022 – Lean Change Mangement, LCM. ID 2205126227

IDIOMAS

Español: Lengua materna

Inglés: Medio

CURSOS PROFESIONALES

- ✓ Diplomado en Desarrollo Tecnología Java y Aplicaciones Web Módulo I y II – Universidad Interamericana de Panamá

CONSORCIO EMDOC, EMDOC, CONSORCIO, Santo Domingo, RD

- ✓ Diplomado en Desarrollo Arquitectura Java y Aplicaciones Web Módulo I- Universidad Interamericana de Panamá
- ✓ Diplomado en Desarrollo de Software Orientado a Objetos bajo Tecnología Java Módulo II - Universidad Interamericana de Panamá
- ✓ CISCO Certified Netowork Associate – Módulo I y II – Universidad Latina de Panamá
- ✓ Introducción a CYBERBUILDER – CIBERNETICA, S. A.
- ✓ Plan de Negocio para emprendedores - INADEH
- ✓ Contabilidad en las organizaciones - INADEH
- ✓ Gestión de Proyectos – INADEH
- ✓ Seminario – Taller "Habilidades de Supervisión para Mandos Medios" - FUNDES
- ✓ Diplomado en Conceptos Básico para la Formación de Estrategias de Gobierno Electrónico - OEA
- ✓ Seminario "Habilidades de Liderazgo para Mujeres Altamente Exitosas" - VALHALA
- ✓ Habilidades del Liderazgo
- ✓ El Ejecutivo Efectivo
- ✓ Servicio al Cliente
- ✓ Habilidades de Ventas
- ✓ Seminario de Inteligencia Emocional
- ✓ Seminario de Negociación
- ✓ Seminario de Técnicas de Comunicación

HABILIDADES/CONOCIMIENTOS GENERALES

- ✓ Liderazgo
- ✓ Conocimiento de la metodología de administración de proyectos PMI V6
- ✓ Conocimientos básicos en SharePoint Portal Server 2007 y 2010
- ✓ Capacidad de trabajo en equipo
- ✓ Capacidad para trabajar bajo presión
- ✓ Disposición a estar siempre actualizado
- ✓ Capacidad para la organización del trabajo
- ✓ Conocimiento en la herramienta de Rational Team Concert
- ✓ Conocimiento básico en BPM/SOA
- ✓ Conocimiento de Norma de EIC/ISO 20000 y prácticas de los estándares de ITIL V3.0

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

3.1.6 Documentos Técnicos

3.1.6.1 Resumen ejecutivo

EXPERTO TECNICO CERTIFICADO EN TECNOLOGIA DE IMPRESIÓN DE TARJETAS DE IDENTIDAD

PAULA HELENA CASTILLO RODRIGUEZ

TECNICO CERTIFICADO EN TECNOLOGIA DE IMPRESIÓN DE TARJETAS DE IDENTIDAD	CERTIFICACION	Detalle de la experiencia
Supervisión de la calidad de la impresión en todos los centros de impresión de cedulas	Se incluye el certificado de Muhlbauer	Dirección General de Registro Civil, Identificación y Cedulación Republica de Ecuador  Técnico responsable de la calidad de impresión de las tarjetas de identidad personal (Cedula). Experto en la calidad de los Documentos de Identidad Personal (Cedula) Dirección General de Registro Civil, Identificación y Cedulación Descripción de la contratación: Adquisición, implementación de un sistema informático para la emisión de documentos de identidad y pasaportes electrónicos y provisión de equipos, suscripciones licencias de software, insumos y servicios conexos para la Dirección General de Registro Civil, Identificación y cedulación (DIGERCIC).

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

		Sistema para la emisión de documentos de identidad personal (cedula) de policarbonato y pasaportes electrónicos, PKI/ National PKD/ICAO PKD, ABIS Vigencia: Fecha 2019 a la fecha **Infraestructura de centro de datos principal y secundario, equipamiento para agencias de atención a nivel nacional y en consulados de Ecuador, para un total de 183 agencias de atención nacional para DIGERCIC y 25 agencias de Ministerio de Relaciones Exteriores y Movilidad Humana (MREMH).** **Este proyecto no incluyo los insumos de libretas de pasaportes.** **No incluyo el material para el Documento de identidad personal.** **Descripción detallada del proyecto:** **Suministro, instalación y configuración de un sistema Web descentralizado para el enrolamiento** **Personalización y emisión de documentos de identidad Personal en Policarbonato (100%) formato ID1 y pasaportes electrónicos (EPass) formato ID3** **Sistema de inspección biométrico automatizado de huellas y rostro (ABIS) para 16 millones de registros.** **Sistema de servicios web para búsqueda 1 a 1 y 1 a N de huellas y rostros integrado al ABIS.**

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

		Capacidad minima de 10 mil a 20 mil búsquedas diarias Infraestructura de llave pública (PKI) y su integración y conexión al Directorio de claves públicas de la OACI, se incluyeron módulos de seguridad (HSM) para el resguardo de llaves. Suministro de infraestructura (hw), licencias, suscripciones de software necesarias para la implementación de un centro de datos primario en alta disponibilidad y un sitio secundario para la recuperación de desastres. Suministro de kits – equipos de captura biométrica, producción y entrega de documentos, ambos en esquema descentralizado. Se incluyo como parte del proyecto la capacitación, transferencia de conocimientos, instalación, configuración, puesta en operación, pruebas unitarias y de integración de los sistemas centrales. Migracion de la base de datos biométrica de más de 13.9 millones de registro. Este contrato incluyo el enrolamiento, personalización y emisión de pasaportes electrónicos en 25 agencias nacionales en Ecuador y 3 externas (Consulado de New York, Madrid y una oficina en Quito). Este contrato también incluyo la emisión en el Ecuador de cedulas de identidad personal en policarbonato en 183 agencias de acuerdo con los lineamientos de la OACI [illegible]. De igual forma incluyo servicios de post implementación, los cuales abarcan soporte técnico,

CONSORCIO EMDOC Santo Domingo, R.D.

		mantenimiento preventivo y correctivo con niveles de servicio de 24x7x365 para todos los componentes del sistema. Importante señalar que como parte de un contrato complementario se contrató una solución de identidad digital y firma electrónica para la ciudadanía.
		TRIBUNAL ELECTORAL DE PANAMA **FABRICA DE DOCUMENTO DE IDENTIDAD PERSONAL (Cedula) +SISTEMA BIOMETRICO DE IDENTIFICACION CIUDADANA (ABIS):** **Año 2016 hasta año 2022** **República de Panamá:** Técnico responsable de la calidad de impresión de las tarjetas de identidad personal (Cedula). Experto en la calidad de los Documentos de Identidad Personal (Cedula) **Descripción del proyecto** **Solución de impresión para el documento de identidad personal panameño (Cedula).** **Contrato N0.24/2016/DS Provisión, Desarrollo de Sistemas tales como Sistema de Gestor de Hardware, gestor de producción, gestor de inventarios, distribución, reportes, entre otros (Impresora de documento de identidad personal) y Suministros de 4,500,000 tarjetas (Documento de**

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

		Identidad Personal) equipamiento tecnológico, aplicativo, insumos y servicio de mantenimiento y soporte para el centro de impresión de documento de identidad personal del Tribunal Electoral de Panamá. Valor aproximado del contrato $.6,519,565.42 seis millones quinientos diecinueve mil, quinientos sesenta y cinco con 42/100 dólares de los Estados Unidos de América. ABIS: Numero de registros soportado el sistema ABIS El volumen es de (10,000,000) diez millones de registros (personas) Suministro, instalación y soporte, mantenimiento y actualización del sistema biométrico de identificación ciudadana (ABIS), para la extracción, conversión y migración de todos los datos del sistema actual a la nueva solución para ser utilizada en la Dirección de Tecnología de la Información y comunicación (DTIC) del Tribunal Electoral de Panamá. Contrato de soporte y mantenimiento para el sistema impresión/emisión.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R D

498

Mühlbauer
High Tech International

CERTIFICATE

Paula Helena Castillo Rodríguez

employee of

GSI INTERNATIONAL, INC

has successfully attended a

CLP 60 Operation & Maintenance Training

at
03-05, 2022
40 HOURS

Mühlbauer
High Tech International

93426 Roding Germany
Phone: +49 9461 952-0
Fax: +49 9461 952-1101
Email: info@muhlbauer.de
Internet: www.muhlbauer.de

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

Curriculum del personal técnico en campo con experiencia en la producción de documentos de identidad nacionales

CONSORCIO EMDOC
EMDOC
CONSORCIO

300

DAVID MERCHAN ECHEVERRIA

DATOS PERSONALES

Telf: 0939005887

C.I: 0930545470

Correo: davidmerchan35@gmail.com

Dirección: Guayaquil, Mucho Lote 1.

Licencia Tipo B

Sexo: Masculino

Edad: 27 años

Nacionalidad: Ecuatoriana

OBJETIVO

Doy importancia a los detalles y me esfuerzo por lograr los objetivos propuestos, de forma independiente y en equipo. Soy confiable, responsable, comunicativo y capaz de realizar cargo que se me asigne.

REFERENCIAS PERSONALES

Ing. Carolina de Delgado
Telf: 0998255661

Psi. Fernanda Aguirre
Telf: 0993344421

Psi. Leslye Cabezas
Telf: 0969879993

EXPERIENCIA PROFESIONAL

SOPORTE TECNICO – GSI INT. INC.

Julio 2024 - Actualidad

(Servicios de impresión a documentos de identificación)

Soporte en sitio a las máquinas de impresión de documentos gubernamentales. Realización de mantenimientos preventivos y correctivos, elaboración de informes técnicos, reparaciones a equipos periféricos y atención a la mesa de ayuda.

Experiencia en la producción de documentos de identidad nacionales, experiencia en impresión, servicios de instalación, soporte y mantenimiento a la infraestructura de impresión y producción de documentos de identidad

AUXILIAR DE COMPRAS - CONSORCIO URVASEO

Marzo 2023 - Junio 2024

(Servicio de recolección de desechos sólidos)

Compras de repuestos mecánicos para las áreas de mantenimiento y metalmecánico, seguimiento a órdenes de compra, control de bodegas a consignación, conocimientos en repuestos para flota pesada y liviana.

BODEGUERO – LABZ

abril 2020 - febrero 2022

(Tratamiento de aguas residuales).

Dirigir y controlar las actividades de recepción y despacho, uso de Buenas Prácticas de Almacenamiento (BPA), manejo de kardex, control de inventarios y supervisión de bodega.

HISTORIAL ACADÉMICO

Universidad Politécnica Salesiana

Ingeniería Mecatrónica (estudios culminados)

- Sólidos conocimientos en control de sistemas mecánicos y electrónicos. Gestión de mantenimientos y costos.

Colegio San Jose La Salle

Bachillerato FIMA

CURSOS

Mecánica a Diesel

Consorcio Urvaseo

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

501

Marketing
Universidad Técnica Particular de Loja

Paquet
Cámara de Comercio Exteri



Ingles B1
Instituto Copei y Cambridge Escrito: 80%
Dialogo: 70%

ISO 9001 2015
Kyrios Consulting

Pocas veces pensamos en lo que tenemos; pero siempre en lo que nos falta.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo

3.1.6 Documentos Técnicos

3.1.6.1 Resumen ejecutivo

TÉCNICO EN CAMPO CON EXPERIENCIA EN LA PRODUCCIÓN DE DOCUMENTOS DE IDENTIDAD NACIONALES MEDIANTE MODELO DESCENTRALIZADO DE IMPRESIÓN.

DAVID MERCHAN

TÉCNICO EN CAMPO CON EXPERIENCIA EN LA PRODUCCIÓN DE DOCUMENTOS DE IDENTIDAD NACIONALES MEDIANTE MODELO DESCENTRALIZADO DE IMPRESIÓN,	**DESCRIPCION DEL ROL**	DETALLE DE LA EXPERIENCIA
Técnico de campo para brindar los Servicios de instalación, soporte y mantenimiento a la infraestructura de impresión a nivel nacional y países en el exterior (en Nueva York (los equipos de Estados Unidos y Canadá) y en Madrid (los equipos de Europa).	Servicios de instalación, soporte y mantenimiento a la infraestructura de impresión a nivel nacional y países en el exterior (reparar en Nueva York (los equipos de Estados Unidos y Canadá) y en Madrid (los equipos de Europa).	Dirección General de Registro Civil, Identificación y Cedulación Republica de Ecuador  Vigencia: Fecha 2019 a la fecha Técnico de campo para para brindar servicios de instalación, soporte y mantenimiento a la Infraestructura de impresión para la producción de documentaos de identidad, pasaportes electrónicos, y la provisión de equipamiento, suscripciones-licencias de software, insumos y servicios conexos en la Republica de Ecuador y en el exterior. **Descripción de la contratación: Adquisición, implementación de un sistema informático para la emisión de documentos de identidad y pasaportes electrónicos y provisión de equipos, suscripciones – licencias de software, insumos y servicios conexos para la Dirección General de Registro Civil, Identificación y cedulación (DIGERCIC).** Sistema para la emisión de documentos de identidad personal (cedula) de policarbonato y pasaportes electrónicos, PKI/ National PKD/ICAO PKD, ABIS Infraestructura de centro de datos principal y secundario, equipamiento para agencias de atención a nivel nacional y en consulados de Ecuador, para un total de 183 agencias de atención nacional para DIGERCIC y 25 agencias de Ministerio de Relaciones Exteriores y Movilidad Humana (MREMH). Descripción detallada del proyecto: Suministro, instalación y configuración de un sistema Web descentralizado para el enrolamiento Personalización y emisión de documentos de identidad Personal en Policarbonato (100%)

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RO

		formato ID1 y pasaportes electrónicos (EPass) formato ID3 Sistema de inspección biométrico automatizado de huellas y rostro (ABIS) para 16 millones de registros. Sistema de servicios web para búsqueda 1 a 1 y 1 a N de huellas y rostros integrado al ABIS. Capacidad mínima de 10 mil a 20 mil búsquedas diarias Infraestructura de llave pública (PKI) y su integración y conexión al Directorio de claves públicas de la OACI, se incluyeron módulos de seguridad (HSM) para el resguardo de llaves. Suministro de infraestructura (HW), licencias, suscripciones de software necesarias para la implementación de un centro de datos primario en alta disponibilidad y un sitio secundario para la recuperación de desastres. Suministro de kits – equipos de captura biométrica, producción y entrega de documentos, ambos en esquema descentralizado. Se incluyo como parte del proyecto la capacitación, transferencia de conocimientos, instalación, configuración, puesta en operación, pruebas unitarias y de integración de los sistemas centrales. Migración de la base de datos biométrica de más de 13.9 millones de registro. Este contrato incluyo el enrolamiento, personalización y emisión de pasaportes electrónicos en 25 agencias nacionales en Ecuador y 3 externas (Consulado de New York, Madrid y una oficina en Quito). Este contrato también incluyo la emisión en el Ecuador de cedulas de identidad personal en policarbonato en 183 agencias de acuerdo con los lineamientos de la OACI 9303. De igual forma incluyo servicios de post implementación, los cuales abarcan soporte técnico, mantenimiento preventivo y correctivo con niveles de servicio de 24x7x365 para todos los componentes del sistema. Importante señalar que como parte de un contrato complementario se contrató una solución de identidad digital y firma electrónica para la ciudadanía. Manejar y configurar impresoras y dispositivos de hardware.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD



David ARCE Flores

- **Dirección:** Conjunto Habitacional Los Libertadores Bq A3 22
- **Celular:** (593) 0982680149
- **Correo electrónico:** oarcef@hotmail.com

Poseo experiencia de más de 20 años en el campo de la informática, gestión deseguridad de la información, gestión de infraestructura de redes, telecomunicaciones, hardware, software; en los que he desempeñado diferentesfunciones relacionadas con planificación y ejecución de proyectos, elaboración de planes de contingencia, continuidad del negocio, implementación de políticasde seguridad, administración de redes, administración de servicios corporativos de red, desarrollo de aplicaciones, implementación y administración de infraestructura de comunicaciones, elaboración de procedimientos, manuales y documentación técnica de diferente índole.

Objetivo:

Aportar con mi experiencia y conocimientos a mejorar los procesos de tecnologíaseguridad informática y de la información, permitiendo a las empresas cumplir sus objetivos en un entono más eficiente y seguro para el cumplimiento de sus proyectos.

David ARCE Flores

CONSORCIO EMDOC Santo Domingo, RD

INSTRUCCIÓN FORMAL:

UNIVERSIDAD AUTONOMA DE QUITO
Ingeniería en Sistemas Informáticos

CENTRO TECNOLOGICO NAVAL
Tecnólogo Naval en Electrónica

INSTITUTO SUPERIOR DE PROFESIONES MEDIAS ESPROMED
Programador de computadoras

COLEGIO TECNICO INDUSTRIAL MIGUEL DE SANTIAGO
Bachiller Técnico en Electromecánica

CURSOS Y SEMINARIOS APROBADOS:

- ***"ADMINISTRACION EN LINUX "*** Dictado en la Escuela Politécnica del Ejército del 6al 13 de Marzo a del 2003, duración 30 horas. Quito Ecuador
- ***"NETWORKING EN LINUX "*** Dictado en la Escuela Politécnica del Ejército del 14 deMarzo a 21 de Marzo del 2003, duración 30 horas. Quito Ecuador
- ***"CURSO DE DISEÑO DE PAGINAS WEB"*** Dictado en el Grupo Tecninegocios el 30de Enero del 2003, duración 100 horas .Quito Ecuador
- ***"SEGURIDAD INFORMATICA y ADMINISTRACIÓN SEGURIDADES LINUX Y CRIPTOGRAFÍA"*** Dictado en el Centro de Tecnología de la Información, el 8 de Enero del 2003, duración 100 horas.
- ***"SEGURIDAD EN REDES LINUX MÓDULO II"*** Dictado por Intser y Avalado por la Universidad Martha Abreu de las Villas de Cuba, 10 Julio del 2003 dictado por MarthaAbreu de la Villas
- ***"PROJECT WEB ACCES".*** Dictado del 17 de Abril al 4 de Abril del 2004, duración 24 horas. Quito-Ecuador.
- ***"ALTIRIS CLIENT MANAGMENT SUITE"*** del 10 de Agosto al 1 de Septiembre del 2004 con duración de 100 hrs. CUMPUEQUPODOS
- ***"CURSO BASICO DE GENEXUS"*** del 21 de Junio al 08 Julio del 2004 en la Universidad Autónoma de Quito UNAQ. Duración 40 horas.
- ***"CURSO BASICO DE PROGRAMACION DE RUTEADORES"*** del 10 al 28 de Mayo2004. Duración 40 horas.
- ***"KASPERSKY SECURITY CONFIGURATION"*** 13 al 30 de Julio del 2004
- ***"CONFIGURACIÓN DE WINDOWS 2003 SERVER, POLITICAS DE ACCESOSBAJO DIRECTORIO ACTIVO E ISA SERVER 2004"*** 9 al 17 de Noviembre 2004.
- ***"CURSO DE ETHICAL HACKER "*** 21 al 22 de Abril del 2006

Flores
ARCHIVO
CONSORCIO EMDOC CONSORCIO Santo Domingo

- ***"SEMINARIO ETHICAL HACKING"*** 16 al 17 de Mayo del 2006

- ***"CISSP BOOT CAMP CERTIFIED INFRAESTRUCTURE SYSTEMS SECURITYPROFESSIONAL"*** 23 al 27 de Abril del 2007

- ***Cisco Certified Networking Administration módulos 1,2,3,4*** *2007 al 2008*
- *Seminario de Implementación y aplicación de* ***"POLITICAS DE SEGURIDAD INFORMATICA"*** 21 de Mayo al 08 de Junio del 2007

- *Seminario teórico práctico para la* ***"PLANEACION ESTRATÉGICA DE TECNOLOGIA INFORMÁTICA" (PETI 2009)*** *Aplicado a los Sistemas de TI.*

- ***"SEMINARIO ITIL V.3 GESTION DE SERVICIOS DE TECNOLOGIAS DE LAINFORMACION"*** 16 Y 17 DE Julio del 2010 dictado por la empresa CAPLAM.

- ***"SEMINARIO ADMINISTRACION DE EQUIPOS DE SEGURIDAD PERIMETRALCHECKPOINT"*** 5 al 9 de Noviembre del 2012 dictado por la empresa AKROS.

- **"CURSO DE MCAFEE INTEGRITY CONTROL"** del 10 al 18 de Febrero del 2015 porla empresa SINERGY TEAM.

- **"CURSO IMPERVA SECURESPHERE ADMINISTRATION 11.0 WEB APPLICATION FIREWALL AND DATABASE SECURITY"** del 10 al 15 de Abril 2015por la empresa EBTEL.

David ARCE Flores

CONSORCIO EMDOC Santo Domingo

EXPERIENCIA PROFESIONAL:

Enero 1999 Hasta febrero 2001	❖ **FUERZA NAVAL** **DIRECCION DE ELECTRONICA COMUNICACIONES Y ARMAMENTO.** **Cargo:** Especialista en mantenimiento de hardware **Funciones desempeñadas:** Planificar, ejecutar y evaluar el mantenimiento preventivo y correctivo del hardware de los repartos de la plaza de Guayaquil.
Febrero 2001 hasta agosto 2008	**FUERZA NAVAL** **CENTRO DE TECNOLOGIA DE LA INFORMACIÓN DE QUITO** **Cargo:** Administrador de la Red Naval de Datos Nodo Norte **Funciones desempeñadas:** Planificación, ejecucion y evaluación de distintos proyectos vinculados a la Red Naval de Datos nodo Norte y los servicios corporativos que ella presta: ❖ Instalación y Configuración de Servidores para los diferentes servicios de la red bajo plataforma Windows 2000, 2003 y Linux Advanced Server. ❖ Implementación de políticas de seguridad bajo el esquema del Directorio Activo para los recursos de la R.N.D Nodo Norte. ❖ Planificación de actividades de la división Centro de Tecnologia de la Información. Administración del personal del Centro Asesoramiento a la Jefatura del Estado Mayor en asuntos de Telecomunicaciones, seguridades y servicios corporativos institucionales ❖ Administración mediante el Directorio Activo de las cuentas de usuarios, equipos, equipos y servicios de la Red. ❖ Implantación, administración y monitoreo del servidor de correo electrónico mediante Exchange Server 2000 y 2003 ❖ Implantación, administración y monitoreo del servidor de Project Server ❖ Implantación, administración y monitoreo del servidor de colaboración basado en SharePoint Team services. ❖ Implantación, administración y monitoreo del servidor de antivirus ❖ Implantación, administración y monitoreo del servidor de aplicaciones remotas mediante Citrix Presentation Server ❖ Elaboración de cronogramas de la División de Redes y Seguridades del CETEIQ. ❖ Planificación y mantenimiento preventivo de los elementos activos y pasivos de la red ❖ Planificación y mantenimiento preventivo de los servidores ❖ Soporte y asesoría a los usuarios finales de la red LAN - WAN en los distintos servicios de la R.N.D. Elaboración de informes y estadísticas de los usuarios, equipos y servicios de la red COGMAR.

David ARCE Flores

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

Agosto 2008 hasta enero 2009	**FUERZA NAVAL** **CENTRO DE TECNOLOGIA DE LA INFORMACIÓN DE QUITO** **Cargo:** Jefe del Centro de Tecnología de la Información de Quito **Funciones desempeñadas:** Planificación, ejecución y control de distintos proyectos vinculados a la Red Naval de Datos y los servicios corporativos que ella presta: ❖ Proyecto de creación de la plataforma de servicios corporativos bajo estructura del Directorio Activo. ❖ Actualización de Sistema de Gestión de Seguridad para la Red Naval de Datos ❖ Planificación de actividades de las divisiones del Centro de Tecnología de la Información. ❖ Administración del personal del Centro Informático ❖ Asesoramiento a la Jefatura del Estado Mayor en asuntos de Telecomunicaciones, seguridades y servicios corporativos institucionales.
Enero 2009 hasta 30 de septiembre 2010	**FUERZA NAVAL** **Cargo:** Jefe de la División de Administración de Recursos Informáticos **Funciones desempeñadas:** Planificación, ejecución y control de distintos proyectos vinculados a la Red Naval de Datos y los servicios corporativos que ella presta: ❖ Actualización de políticas y procedimientos de Seguridad para la Red Naval de Datos ❖ Planificación y ejecución de proyectos. ❖ Administración del personal de la División ❖ Asesoramiento a la Jefatura en asuntos de Informática, seguridad, Telecomunicaciones, planificación de servicios corporativos institucionales.
Septiembre 2010 hasta marzo 2012	**BNR Sistemas** **Cargo: Gerente Técnico** **Funciones desempeñadas:** ❖ Consultoría IT a empresas ❖ Asesoría en Seguridades, Redes de Datos, Comunicaciones



	❖ Implementación de servicios corporativos de Red ❖ Elaboración de documentación técnica: Planes de Contingencia y Seguridad, Planes Estratégicos de Tecnología de la Información.
Abril 2012 hasta la mayo 2015	**DINARDAP** **Cargo: Especialista de Seguridad Informática** **Funciones desempeñadas:** ❖ Colaborar dentro de la Dirección de Seguridad Informática para la implementación del Sistema de Gestión de Seguridad Informática. ❖ Recopilar datos de los procesos y procedimientos de las diferentes áreas con el fin de analizarlos y verificar incidencias de seguridad (riesgos o violaciones). ❖ Realizar el análisis de las vulnerabilidades de la red interna y perimetral de la Dirección Nacional de Registro de Datos, proporiendo y coordinando la implementación de las alternativas de solución y los elementos de seguridad necesarios para la transmisión de datos en forma segura en todas las capas que componen dicha red. ❖ Coordinar con la Dirección de Tecnología y Desarrollo la configuración segura de los elementos activos de red, servidores y servicios presentes en la infraestructura de la Direccion Nacional de Registro de Datos Públicos. ❖ Administrar los elementos de seguridad definidos para la granja de servidores, equipos activos de red y la capa perimetral de datos. ❖ Colaborar y coordinar con la Dirección de Tecnología y Desarrollo la implementación de políticas de configuración segura para los servicios de red tales como DHCP (Dynamic Host Configuration Protocol), DNS (Domain Name System), SMTP (Simple Mail Transfer Protocol), VoIP, y demás servicios instalados en la Institución. ❖ Administración del Open ERP para la gestión de calidad ISO 9000:2008, obtenida por la Institución. ❖ Administración del Sistema de Vigilancia, Monitoreo, sensores y alarmas implementado a nivel Nacional. ❖ Elaborar la documentación técnica concerniente a los equipos e implementación de servicios a cargo. ❖ Elaboración de especificaciones técnicas para los proyectos llevados a cabo por la Dirección de Seguridad Informática. ❖ Generación de documentación técnica sobre los mecanismos de seguridad implementados.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

Junio 2015 hasta 31 marzo 2016	**DINARDAP** **Cargo: Director de Seguridad Informática** **Funciones desempeñadas:** ❖ Elaborar la planificación anual de la Dirección Desarrollar e implementar mecanismos de seguridad que permitan garantizar el aseguramiento de la información institucional y la plataforma informática. ❖ Asesorar a las autoridades en materia de seguridad informática y seguridad de la información. ❖ Investigar y mantenerse actualizado en materia de procesos y procedimientos de tecnología y seguridad informática, así como de proyectos de seguridad informática a fin de implementar las actualizaciones y cambios necesarios. ❖ Velar por el cumplimiento de normas, políticas, estándares y procedimientos para el aseguramiento de la información al interior de la Institución. ❖ Participar en el diseño de planes de contingencia, tecnológicos e informáticos, para el mantenimiento de la seguridad de la información Institucional. ❖ Gestionar los incidentes de seguridad informática de la institución. ❖ Elaborar informes de valoración y mitigación de riesgos e incidencias de la plataforma tecnológica. ❖ Revisar y aprobar los componentes de seguridad en proyectos tecnológicos de la institución. ❖ Elaborar informes de la gestión de seguridad de la plataforma SINARDAP. ❖ Elaborar especificaciones técnicas para el desarrollo de Programas y Proyectos de Inversión en cuanto a seguridad informática del registro de datos. ❖ Supervisar el soporte técnico en Seguridad informática a usuarios internos, externos y a nivel regional

David ARCE Flores

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

Abril 2016 hasta agosto 2018	**Consultor Técnico Freelance** **Funciones desempeñadas:** ❖ Soporte y consultoría sobre proyectos de seguridad informática, soluciones de Networking, gestión de infraestructura y procesos. ❖ Implementación de servicios corporativos de Red. Correo electrónico, firewall perimetral, DNS, DHCP, antivirus, portales web, implementación de plataformas educativas basadas en Moodle, entre otros. ❖ Soporte y mantenimiento de servidores y redes de datos. ❖ Elaboración de documentación técnica, planes de contingencia y mejores prácticas basadas en ITIL.
Septiembre 2018 hasta julio 2019	**Coordinador de Sistema Cámara de Comercio Ecuatoriano Americana** **Funciones desempeñadas:** ❖ Implementación de servicios corporativos de Red. Correo electrónico, firewall perimetral, DNS, DHCP, antivirus, portales web. ❖ Soporte y mantenimiento de servidores y redes de datos ❖ Soporte tecnológico a eventos
Julio 2019 a septiembre 2020	**Director de Tecnología de la Presidencia de la República** **Funciones desempeñadas:** ❖ Dirigir la ejecución del Plan Estratégico de Tecnologías de Información (PETI) alineado al Plan Estratégico Institucional; ❖ Gestionar los procesos de tecnologías de la información y comunicaciones; ❖ Planificar y ejecutar la implementación de nuevas tecnologías de la Información; ❖ Gestionar la adopción de estándares, metodologías, arquitecturas, sistemas e infraestructuras adecuadas a las necesidades institucionales; ❖ Coordinar el cumplimiento de la normativa gubernamental en materia de TIC's y seguridad informática; ❖ Definir e implementar políticas y procedimientos para la asistencia y soporte técnico, cambio, renovación cambio y renovación continua de software, hardware, capacidad, disponibilidad, continuidad, seguridad informática de los sistemas y servicios tecnológicos de la institución; ❖ Dirigir, implementar y monitorear la ejecución planes, programas y proyectos de tecnologías de la información y comunicación; ❖ Proveer servicios tecnológicos para solventar las necesidades institucionales internas referentes a comunicaciones, infraestructura, equipamiento informático de usuario final, aplicaciones, software, soporte técnico y atención a eventos institucionales; ❖ Coordinar la elaboración y ejecución de inventario y plan de mantenimiento de la plataforma de servidores, almacenamiento, respaldos, comunicaciones, aplicativos, seguridades y equipos de usuario final de la institución; ❖ Dirigir e implementar el plan de seguridad de la informática

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

	❖ Garantizar la disponibilidad, continuidad, operatividad y mecanismos de seguridad informática de los servicios tecnológicos y sus respetivos planes de contingencias; ❖ Asesorar en los procesos de contratación referentes a tecnologíade la información de la institución y elaborar la documentación técnica habilitante necesaria para su ejecución; ❖ Gestionar la elaboración de manuales e instructivos técnicos de capacitación, operación, usuario, administración y paso a producción de las aplicaciones; ❖ Gestionar convenios institucionales de transferencias tecnológicas; ❖ Coordinar la administración, supervisión de los contratos de las plataformas tecnológicas de hardware, software y servicios tecnológicos; ❖ Asegurar la calidad en la implementación de aplicativos, software, hardware, o servicios tecnológicos desarrollados o adquiridos a través de la ejecución de sus respectivas pruebas; ❖ Gestionar la atención a incidentes y problemas de plataformas de hardware, software, redes de datos, servicios tecnológicos y de seguridad informática escalados por los niveles de soporte establecidos
Septiembre 2020 hasta Octubre 2022	**Consultor Técnico Freelance** **Funciones desempeñadas:** ❖ Soporte y consultoría sobre proyectos de ciberseguridad, soluciones de Networking, gestión de infraestructura, servicios de red y procesos. ❖ Implementación de servicios corporativos de Red. Correo electrónico, firewall perimetral, DNS, DHCP, antivirus, portales web, implementación de plataformas educativas basadas en Moodle, entre otros. ❖ Soporte y mantenimiento de servidores y redes de datos. ❖ Elaboración de documentación técnica, planes de contingencia y mejores prácticas basadas en ITIL.
Octubre 2022 hasta la presente	**Jefe de Tecnología GSI International INC** **Funciones desempeñadas:** ❖ Gestión de Infraestructura interna y de los Proyectos de la empresa ❖ Gestión del soporte técnico de la empresa ❖ Gestión de soporte técnico en los proyectos de la DIGERCIC brindando servicios de instalación, soporte y mantenimiento a la infraestructura de impresión para la producción de documentos de identidad a nivel nacional, incluyendo equipos tecnológico e impresoras. ❖ Gestión de aspectos de ciberseguridad,soluciones de Networking, gestión de infraestructura, servicios de red y procesos IT internos. ❖ Implementación y gestión de servicios corporativos de Red. ❖ Elaboración de documentación técnica

David ARCE Flores

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

3.1.6 Documentos Técnicos

3.1.6.1 Resumen ejecutivo

TÉCNICO EN CAMPO CON EXPERIENCIA EN LA PRODUCCIÓN DE DOCUMENTOS DE IDENTIDAD NACIONALES MEDIANTE MODELO DESCENTRALIZADO DE IMPRESIÓN,

DARIO XAVIER COYAGO ARCE

TÉCNICO EN CAMPO CON EXPERIENCIA EN LA PRODUCCIÓN DE DOCUMENTOS DE IDENTIDAD NACIONALES MEDIANTE MODELO DESCENTRALIZADO DE IMPRESIÓN,	**ROL**	**DETALLE DE LA EXPERIENCIA**
Técnico de campo con experiencia en producción de documentaos de identidad, pasaportes electrónicos, y la provisión de equipamiento, suscripciones-licencias de software, insumos y servicios conexos para la Dirección General de Registro Civil Identificación y cedulación (DIGERCIC)	Servicios de instalación, soporte y mantenimiento a la infraestructura de impresión a nivel nacional y países en el exterior (reparar en Nueva York (los equipos de Estados Unidos y Canadá) y en Madrid (los equipos de Europa).	**Dirección General de Registro Civil, Identificación y Cedulación** **Republica de Ecuador**  Vigencia: Fecha 2019 a la fecha Técnico de campo para para brindar servicios de instalación, soporte y mantenimiento a la infraestructura de impresión para la **producción de documentaos de identidad, pasaportes electrónicos, y la provisión de equipamiento, suscripciones-licencias de software, insumos y servicios conexos en la Republica de Ecuador y en el exterior.** Descripción de la contratación: Adquisición, implementación de un sistema informático para la emisión de documentos de identidad y pasaportes electrónicos y provisión de equipos, suscripciones –

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo - ECUADOR

		licencias de software, insumos y servicios conexos para la Dirección General de Registro Civil, Identificación y cedulación (DIGERCIC). Sistema para la emisión de documentos de identidad personal (cedula) de policarbonato y pasaportes electrónicos, PKI/ National PKD/ICAO PKD, ABIS **Infraestructura de centro de datos principal y secundario, equipamiento para agencias de atención a nivel nacional y en consulados de Ecuador, para un total de 183 agencias de atención nacional para DIGERCIC y 25 agencias de Ministerio de Relaciones Exteriores y Movilidad Humana (MREMH).** **Descripción detallada del proyecto:** **Suministro, instalación y configuración de un sistema Web descentralizado para el enrolamiento** **Personalización y emisión de documentos de identidad Personal en Policarbonato (100%) formato ID1 y pasaportes electrónicos (EPass) formato ID3** **Sistema de inspección biométrico automatizado de huellas y rostro (ABIS) para 16 millones de registros.** **Sistema de servicios web para búsqueda 1 a 1 y 1 a N de huellas y rostros integrado al ABIS.**

CONSORCIO EMDOC
EMDOC CONSORCIO
Santo Domingo, R.D.

		Capacidad mínima de 10 mil a 20 mil búsquedas diarias Infraestructura de llave pública (PKI) y su integración y conexión al Directorio de claves públicas de la OACI, se incluyeron módulos de seguridad (HSM) para el resguardo de llaves. Suministro de infraestructura (HW), licencias, suscripciones de software necesarias para la implementación de un centro de datos primario en alta disponibilidad y un sitio secundario para la recuperación de desastres. Suministro de kits – equipos de captura biométrica, producción y entrega de documentos, ambos en esquema descentralizado. Se incluyo como parte del proyecto la capacitación, transferencia de conocimientos, instalación, configuración, puesta en operación, pruebas unitarias y de integración de los sistemas centrales. Migración de la base de datos biométrica de más de 13.9 millones de registro. Este contrato incluyo el enrolamiento, personalización y emisión de pasaportes electrónicos en 25 agencias nacionales en Ecuador y 3 externas (Consulado de New York, Madrid y una oficina en Quito). Este contrato también incluyo la emisión en el

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

		Ecuador de cedulas de identidad personal en policarbonato en 183 agencias de acuerdo con los lineamientos de la OACI 9303. De igual forma incluyo servicios de post implementación, los cuales abarcan soporte técnico, mantenimiento preventivo y correctivo con niveles de servicio de 24x7x365 para todos los componentes del sistema. Importante señalar que como parte de un contrato complementario se contrató una solución de identidad digital y firma electrónica para la ciudadanía. Manejar y configurar impresoras y dispositivos de hardware.



517

ESTERVINA DISLA UTATE

Ingeniera de Sistemas

Excelentes relaciones públicas. Habilidades de persuasión, toma de decisiones y liderazgo. Estrategia. Dirección de Proyectos. Conocimiento de programación. Excelente visión de proyección. Facilidad de aprendizaje. Trabajo con equipos multiculturales de forma remota. Más de 6 años de experiencia manejando equipos y procesos con fines exitosos.

EXPERIENCIA

Ago 2013 - Actualmente

Gerente de Operaciones y Tecnico de Campo
GSI Internacional

Experiencia en la producción de documentos de Identidad nacional, mediante modelo descentralizado de impresión, su experiencia incluye: servicio de instalación, Soporte y mantenimiento de a la infraestructura de impresión. Participo en la Instalación de Pasaporte y cedulas de Identidad de la Rep. de Ecuador.

Planificación y organización: Desarrollar estrategias para mejorar la eficiencia operativa del departamento, asignar recursos adecuados y establecer objetivos claros.

Gestión de personal: Contratar, capacitar, supervisar y motivar al personal de operaciones para garantizar un rendimiento óptimo.

Control de calidad: Supervisar y mantener los estándares de calidad en los productos o servicios de la empresa, implementando procesos de control de calidad y resolviendo problemas relacionados con la calidad.

Mejora continua: Identificar áreas de mejora en los procesos operativos y desarrollar e implementar iniciativas para aumentar la eficiencia, reducir costos y mejorar la calidad.

Santo Domingo
Mar 2021 - Ago 2013

Gerente de Proyectos
GSI Internacional

Gestión de proyectos de índole documental, automatización de procesos con herramientas BPM. Pudiendo destacar los siguientes proyectos dentro del sector:

- Banreservas: Gestión del proyecto para la provisión de plataforma Bizagi para la automatización de los procesos Tarjeta de Crédito, Préstamos de Consumo e integración Motor de Decisiones y Excepciones.
- BGR: Gestion de proyecto para la provisión de plataforma Bizagi para la automatización de estos procesos Core de la institución.
- Banco Promerica: Gestion de proyecto para la provisión de plataforma Bizagi para la automatización de los procesos Tarjeta de Crédito, Préstamos de Consumo sin garantía y Motor de Decisiones y Excepciones.

Santo Domingo, República Dominicana
Ene 2019 - Feb 2021

Project Manager
Alcoh Dominicana

- Gestión de proyectos desde que representan una oportunidad para la empresa hasta la entrega en el area de servicios. Siendo responsable en la metodología a utilizar.
- Participación en proyectos de índoles tecnológicas, como implementación de parques de impresoras, gestores documentales, sistemas de vigilancia, entre en diversos sectores.
- Gestión de un promedio de 4 propuestas por mes.

Santo Domingo, República Dominicana
May 2019 - Jun 2021

Coordinadora de Proyectos
GSI Internacional

- Encargada de la gestión de proyectos, recursos y alcance de los mismos.
- Gestión de diversos proyectos, tanto en el sector financiero o de la banca como en el sector público,

INFORMACIÓN DE CONTACTO

Email
e.disla.utate@gmail.com

Dirección
Av. Isabel Aguiar, Residencial Isabel Aguiar 301, Edif. 5, Apto 504, Sto. Dgo. Norte

Teléfono
(809) 651-1291

Fecha de nacimiento
18 Ene. 1991

Nacionalidad
Dominicana

Enlace
https://www.linkedin.com/in/estervina-disla-utate-4b6a6b67

HABILIDADES

- Trabajo en Equipo
- Manejo de equipos diversos
- Comunicación Asertiva
- Resolución de Conflictos
- Resiliencia
- Liderazgo
- Orientación a resultados
- Trabajo Remoto

IDIOMAS

Español
nativo

Spanish
native

CONSORCIO EMDOC
EMDOC CONSORCIO
Santo Domingo, RD

3.1.6 Documentos Técnicos

3.1.6.1 Resumen ejecutivo

TÉCNICO EN CAMPO CON EXPERIENCIA EN LA PRODUCCIÓN DE DOCUMENTOS DE IDENTIDAD NACIONALES MEDIANTE MODELO DESCENTRALIZADO DE IMPRESIÓN.

ESTERVINA DISLA UTATE

TÉCNICO EN CAMPO CON EXPERIENCIA EN LA PRODUCCIÓN DE DOCUMENTOS DE IDENTIDAD NACIONALES MEDIANTE MODELO DESCENTRALIZADO DE IMPRESIÓN,	**DESCRIPCION DEL ROL**	**DETALLE DE LA EXPERIENCIA**
Técnico de campo para brindar los Servicios de instalación, soporte y mantenimiento a la infraestructura de impresión a nivel nacional y países en el exterior (en Nueva York (los equipos de Estados Unidos y Canadá) y en Madrid (los equipos de Europa).	Servicios de instalación, soporte y mantenimiento a la infraestructura de impresión a nivel nacional y países en el exterior (reparar en Nueva York (los equipos de Estados Unidos y Canadá) y en Madrid (los equipos de Europa).	**Dirección General de Registro Civil, Identificación y Cedulación** **Republica de Ecuador**  Vigencia: Fecha 2019 a la fecha Técnico de campo para para brindar servicios de instalación, soporte y mantenimiento a la infraestructura de impresión para la producción de documentaos de identidad, pasaportes electrónicos, y la provisión de equipamiento, suscripciones-licencias de software, insumos y servicios conexos en la Republica de Ecuador y en el exterior. Descripción de la contratación: Adquisición, implementación de un sistema informático para la emisión de documentos de identidad y pasaportes electrónicos y provisión de equipos, suscripciones – licencias de software, insumos y servicios conexos para la Dirección General de Registro Civil, Identificación y cedulación (DIGERCIC). Sistema para la emisión de documentos de identidad personal (cedula) de policarbonato y pasaportes electrónicos, PKI/ National PKD/ICAO PKD, ABIS Infraestructura de centro de datos principal y secundario, equipamiento para agencias de atención a nivel nacional y en consulados de Ecuador, para un total de 183 agencias de atención nacional para DIGERCIC y 25 agencias del Ministerio de Relaciones Exteriores y Movilidad Humana (MREMH). Descripción detallada del proyecto: Suministro, instalación y configuración de un sistema Web descentralizado para el enrolamiento



		Personalización y emisión de documentos de identidad Personal en Policarbonato (100%) formato ID1 y pasaportes electrónicos (EPass) formato ID3 Sistema de inspección biométrico automatizado de huellas y rostro (ABIS) para 16 millones de registros. Sistema de servicios web para búsqueda 1 a 1 y 1 a N de huellas y rostros integrado al ABIS. Capacidad mínima de 10 mil a 20 mil búsquedas diarias Infraestructura de llave pública (PKI) y su integración y conexión al Directorio de claves públicas de la OACI, se incluyeron módulos de seguridad (HSM) para el resguardo de llaves. Suministro de infraestructura (HW), licencias, suscripciones de software necesarias para la implementación de un centro de datos primario en alta disponibilidad y un sitio secundario para la recuperación de desastres. Suministro de kits – equipos de captura biométrica, producción y entrega de documentos, ambos en esquema descentralizado. Se incluyo como parte del proyecto la capacitación, transferencia de conocimientos, instalación, configuración, puesta en operación, pruebas unitarias y de integración de los sistemas centrales. Migración de la base de datos biométrica de más de 13.9 millones de registro. Este contrato incluyo el enrolamiento, personalización y emisión de pasaportes electrónicos en 25 agencias nacionales en Ecuador y 3 externas (Consulado de New York, Madrid y una oficina en Quito). Este contrato también incluyo la emisión en el Ecuador de cedulas de identidad personal en policarbonato en 183 agencias de acuerdo con los lineamientos de la OACI 9303. De igual forma incluyo servicios de post implementación, los cuales abarcan soporte técnico, mantenimiento preventivo y correctivo con niveles de servicio de 24x7x365 para todos los componentes del sistema. Importante señalar que como parte de un contrato complementario se contrató una solución de identidad digital y firma electrónica para la ciudadanía. Manejar y configurar impresoras y dispositivos de hardware.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

		TRIBUNAL ELECTORAL DE PANAMA FABRICA DE DOCUMENTO DE IDENTIDAD PERSONAL (Cédula) +SISTEMA BIOMETRICO DE IDENTIFICACION CIUDADANA (ABIS): Año 2016 hasta año 2022 República de Panamá:  Técnico responsable del soporte a nivel nacional y en el extranjero, con experiencia en la producción de documentos de identidad nacional, incluyendo el soporte de equipos tecnológicos y las impresoras. Descripción del proyecto Solución de impresión para el documento de identidad personal panameño (Cédula). Contrato NO.24/2016/DS Provisión, Desarrollo de Sistemas tales como Sistema de Gestor de Hardware, gestor de producción, gestor de inventarios, distribución, reportes, entre otros (Impresora de documento de identidad personal) y Suministros de 4,500,000 tarjetas (Documento de Identidad Personal) equipamiento tecnológico, aplicativo, insumos y servicio de mantenimiento y soporte para el centro de impresión de documento de identidad personal del Tribunal Electoral de Panamá. Valor aproximado del contrato $.6,519,565.42 seis millones quinientos diecinueve mil, quinientos sesenta y cinco con 42/100 dólares de los Estados Unidos de América. ABIS: Numero de registros soportado el sistema ABIS El volumen es de (10,000,000) diez millones de registros (personas) Suministro, instalación y soporte, mantenimiento y actualización del sistema biométrico de identificación ciudadana (ABIS), para la extracción, conversión y migración de todos los datos del sistema actual a la nueva solución para ser utilizada en la Dirección de Tecnología de la Información y comunicación (DTIC) del Tribunal Electoral de Panamá. Contrato de soporte y mantenimiento para el sistema impresión/emisión.



KERLY K. PINILLA C.

521

CÉDULA: 6-705-1584, CUIDADANA PANAMEÑA, CASADA, NACIDA EL 3 DE MARZO DE 1981 EN LA CIUDAD DE CHITRÉ, PROVINCIA DE HERRERA, PANAMÁ.

OBJETIVO

Trabajar en el ambiente de una Empresa en la cual pueda proporcionar cambios tecnológicos y culturales que promuevan su productividad y junto con un exitoso equipo de trabajo, contribuir al desarrollo integral de la misma. Continuar superándome en el aspecto personal, laboral y profesional.

EXPERIENCIA

- Actualmente estoy trabajando en GSI International INC., en el Área de Tecnología; Encargada de Administrar la Base De Datos Oracle, Programación e Instalación de Software. Año 2009.
- Apoyo técnico de campo para brindar servicios de instalación, soporte y mantenimiento a la infraestructura de impresión para la producción de documentaos de identidad, pasaportes electrónicos, y la provisión de equipamiento, suscripciones-licencias de software, insumos y servicios conexos en la Republica de Ecuador y en el exterior.
- Arango Software International, Área de Desarrollo. Años 2005 - 2009.
- TV Shopping, Área de Ventas y Tele mercadeo. Enero-Junio 2005.
- Conexiones Panamá, Área de Tele mercadeo. Octubre-Noviembre 2004.
- MDM Securities, S.A. Practicante - Soporte Técnico. Control e Instalación de Software, Mantenimiento y Reparación de Hardware. Mayo – Junio 2004.
- Súper 99 S.A. Empleado Eventual de Administración de Software de Lectoras de Códigos de Barra en el Inventario de la ciudad de Chitré. Enero 2003.
- Empleado Eventual en el Inventario de la Distribuidora de Productos Farmacéuticos SmithKline Beecham. Prov. Panamá. Septiembre 1999.

FORMACIÓN

- Maestría en Gerencia de Base de Datos, Universidad Latina de Panamá. Año 2016.
- Licenciatura Ingeniería en Sistemas Computacionales, Universidad Tecnológica de Panamá. Año 2006.

HABILIDADES

- Capacidad de Comunicación Verbal y Escrita. - Capacidad de trabajo en equipo y bajo presión. - Orientación hacia el cumplimiento de tareas específicas. - Rápida captación de conocimientos. - Facilidad para enfocar mis Fortalezas en pro de una meta. - Facilidad para la docencia.

HABILIDADES TÉCNICAS

- Conocimiento del Idioma Inglés a Nivel Técnico - Conocimientos en Herramientas de Office - Conocimientos en Base de Datos: Access, SQL Server Oracle. - Conocimientos de programación en: Java, Visual Basic 6.0, C++, Pascal y PL/Sql - Diseño asistidos por computadora Macromedia Dreamweaver y FrontPage (Páginas Web). Conocimientos en Herramientas, Oracle (Forms y Reports) 6i – 9i – 10g – 11g – 12c, Toad, sqldeveloper - Análisis y Programación de sistemas. - Conocimientos en Herramientas de Inteligencia de negocios.

CONSORCIO EMDOC
EMDOC
CONSORCIO
S.D. R.D.

CONFERENCIAS Y SEMINARIOS

- Curso de QlikSense de 16 Horas. Año.2017
- Capacitación de Auditor Interno de 8 Horas. Año 2017.
- Capacitación en Webservice WSO2 Middleware e Intalo BMP de 40 Horas. Año 2012.
- Curso de QlikView de 16 Horas. Año 2012.
- Seminario de Fundamentos de la Tecnología de Tarjetas Inteligentes de 16 Horas. Año 2011
- Curso de Sensibilización para Calidad de ISO 9001. Año 2010.
- Curso de Administración Básica de Base de Datos Oracle 10g de 40 Horas. Año 2010
- Taller de Cuerdas Facilitadores del Istmo. Año 2010.
- Capacitación del Negocio de Servicios de Transportes Centroamericanos Módulos de Licencias, Placas, RUVM, PYD, Transporte, Juzgados, Infracciones, Auto Escuela, Revisados, Comunes y Boleteras Electrónicas y Herramientas de Desarrollo para SEDOS (Sistema de Emisión de Documentos Seguros) y SETRES(Sistema de Tramites Registrables Seguros) – 2009 -2010.
- Capacitación del Negocio Bancario (Contabilidad Bancaria, Abanks Módulos de Cuentas de Ahorro, Cuentas Corrientes, Depósitos a Plazo, Prestamos, Líneas Financieras, Mercado de Dinero, Mesa de Cambio, Garantías) y Herramientas de desarrollo para Oracle – 2005 -2006
- Conferencia sobre Sistemas Operativos de uso Empresarial y Redes. (UTP) Año 2003
- Taller de Introducción a la Firma Digital Uso de Outlook para Correo Electrónico Seguro.(SENACYT) Centro de Firma Digital. Año 2003.
- Primer Congreso de Ingeniería en Azuero. El Avance Tecnológico como Herramienta de Desarrollo Humano: "Hacia un Incremento de la Productividad y la Optimización de los Recursos. (UTP) Año 2002
- Curso de Capacitación dirigido a "Manipuladores de Alimentos y Operarios de Establecimientos de Interés Sanitario" de ocho horas. Año 2001.
- Ciclo de Conferencias en la V Semana de la Ingeniería Ciencia y Tecnología para el Desarrollo Sostenible. (UTP) Año 2000.
- Seminario del Programa Capacitación para Jóvenes para el Primer Trabajo para el Proyecto de Empresas de ciento sesenta horas. Ministerio de Trabajo y Desarrollo (MITRADEL). Año 2000.
- Seminario del Programa Capacitación para Jóvenes para el Primer Trabajo de 80 horas. Ministerio de Trabajo y Desarrollo (MITRADEL). Año 2000.

ÁREAS DE CRECIMIENTO

- Profesional

- Gerencia en Informática. - Desarrollo de aplicaciones web. - Administración de Bases de Datos distribuidas. Gerencia de Proyectos. – Consultoría Informática.
- Motivación del Personal que colabora conmigo en Proyectos del área de sistemas. - Creación de Micro empresas.

CONSORCIO EMDOC
EMDOC CONSORCIO
Santo Domingo, RD

3.1.6 Documentos Técnicos

3.1.6.1 Resumen ejecutivo

TÉCNICO EN CAMPO CON EXPERIENCIA EN LA PRODUCCIÓN DE DOCUMENTOS DE IDENTIDAD NACIONALES MEDIANTE MODELO DESCENTRALIZADO DE IMPRESIÓN.

KERLY K. PINILLA C

TÉCNICO EN CAMPO CON EXPERIENCIA EN LA PRODUCCIÓN DE DOCUMENTOS DE IDENTIDAD NACIONALES MEDIANTE MODELO DESCENTRALIZADO DE IMPRESIÓN	**DESCRIPCION DEL ROL**	**DETALLE DE LA EXPERIENCIA**
Técnico de campo para brindar los Servicios de instalación, soporte y mantenimiento a la infraestructura de impresión a nivel nacional y países en el exterior (en Nueva York (los equipos de Estados Unidos y Canadá) y en Madrid (los equipos de Europa).	Servicios de instalación, soporte y mantenimiento a la infraestructura de impresión a nivel nacional y países en el exterior (reparar en Nueva York (los equipos de Estados Unidos y Canadá) y en Madrid (los equipos de Europa).	**Dirección General de Registro Civil, Identificación y Cedulación** Republica de Ecuador  Vigencia: Fecha 2019 a la fecha Técnico de campo para para brindar servicios de instalación, soporte y mantenimiento a la infraestructura de impresión para la producción de documentaos de identidad, pasaportes electrónicos, y la provisión de equipamiento, suscripciones-licencias de software, insumos y servicios conexos en la Republica de Ecuador y en el exterior. Descripción de la contratación: Adquisición, implementación de un sistema informático para la emisión de documentos de identidad y pasaportes electrónicos y provisión de equipos, suscripciones – licencias de software, insumos y servicios conexos para la Dirección General de Registro Civil, Identificación y cedulación (DIGERCIC).

EMDOC DIGERCIC Santo Domingo, R.D.

		Sistema para la emisión de documentos de identidad personal (cedula) de policarbonato y pasaportes electrónicos, PKI/ National PKD/ICAO PKD, ABIS Infraestructura de centro de datos principal y secundario, equipamiento para agencias de atención a nivel nacional y en consulados de Ecuador, para un total de 183 agencias de atención nacional para DIGERCIC y 25 agencias de Ministerio de Relaciones Exteriores y Movilidad Humana (MREMH). Descripción detallada del proyecto: Suministro, instalación y configuración de un sistema Web descentralizado para el enrolamiento Personalización y emisión de documentos de identidad Personal en Policarbonato (100%) formato ID1 y pasaportes electrónicos (EPass) formato ID3 Sistema de inspección biométrico automatizado de huellas y rostro (ABIS) para 16 millones de registros. Sistema de servicios web para búsqueda 1 a 1 y 1 a N de huellas y rostros integrado al ABIS. Capacidad mínima de 10 mil a 20 mil búsquedas diarias Infraestructura de llave pública (PKI) y su integración y conexión al Directorio de claves públicas de la OACI, se incluyen módulos de seguridad (HSM) para el resguardo de llaves. Suministro de Infraestructura (HW), licencias, suscripciones de.

CONSORCIO EMDOC
EMDOC
CONSORCIO

		software necesarias para la implementación de un centro de datos primario en alta disponibilidad y un sitio secundario para la recuperación de desastres. Suministro de kits – equipos de captura biométrica, producción y entrega de documentos, ambos en esquema descentralizado. Se incluyo como parte del proyecto la capacitación, transferencia de conocimientos, instalación, configuración, puesta en operación, pruebas unitarias y de integración de los sistemas centrales. Migración de la base de datos biométrica de más de 13.9 millones de registro. Este contrato incluyo el enrolamiento, personalización y emisión de pasaportes electrónicos en 25 agencias nacionales en Ecuador y 3 externas (Consulado de New York, Madrid y una oficina en Quito). Este contrato también incluyo la emisión en el Ecuador de cedulas de identidad personal en policarbonato en 183 agencias de acuerdo con los lineamientos de la OACI 9303. De igual forma incluyo servicios de post implementación, los cuales abarcan soporte técnico, mantenimiento preventivo y correctivo con niveles de servicio de 24x7x365 para todos los componentes del sistema. Importante señalar que como parte de un contrato complementario se contrató una solución de identidad digital y firma electrónica para la ciudadanía.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

		Manejar y configurar impresoras y dispositivos de hardware.
		TRIBUNAL ELECTORAL DE PANAMA FABRICA DE DOCUMENTO DE IDENTIDAD PERSONAL (Cedula) +SISTEMA BIOMETRICO DE IDENTIFICACION CIUDADANA (ABIS): Año 2016 hasta año 2022 República de Panamá:  Técnico responsable de la calidad de impresión de las tarjetas de identidad personal (Cedula). Experto en la calidad de los Documentos de Identidad Personal (Cedula) Descripción del proyecto Solución de impresión para el documento de identidad personal panameño (Cedula). Contrato N0.24/2016/DS Provisión, Desarrollo de Sistemas tales como Sistema de Gestor de Hardware, gestor de producción, gestor de inventarios, distribución, reportes, entre otros (Impresora de documento de identidad personal) y Suministros de 4,500,000 tarjetas (Documento de Identidad Personal) equipamiento tecnológico, aplicativo, insumos y servicio de mantenimiento y soporte para el centro de impresión de documento de

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

		identidad personal del Tribunal Electoral de Panamá. Valor aproximado del contrato $.6,519,565.42 seis millones quinientos diecinueve mil, quinientos sesenta y cinco con 42/100 dólares de los Estados Unidos de América. ABIS: Numero de registros soportado el sistema ABIS El volumen es de (10,000,000) diez millones de registros (personas) Suministro, instalación y soporte, mantenimiento y actualización del sistema biométrico de identificación ciudadana (ABIS), para la extracción, conversión y migración de todos los datos del sistema actual a la nueva solución para ser utilizada en la Dirección de Tecnología de la Información y comunicación (DTIC) del Tribunal Electoral de Panamá. Contrato de soporte y mantenimiento para el sistema impresión/emisión.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

528



Curriculum Vitae

NIXON PAUL ESPINOZA NOBOA

Datos Personales

Dirección: 10 DE AGOSTO ESQUINA y 2 ENERO, Sector Guala

Teléfono (s): 0993720343 - 062545052 - 0994591476

Cédula de identidad: 1004003313

Correo electrónico: nixon19paul@gmail.com

Ciudad / Provincia / QUITO / PICHINCHA / ECUADOR

Instrucción Formal

TERCER NIVEL **INGENIERO EN MECATRONICA**

(7 AÑOS) ESCUELA POLITECNICA DEL EJERCITO

Vocación / Subactividades:

Oficio: POLIFUNCIONALES

Descripción: EMPRENDIMIENTO VENTA PRODUCTOS LIMPIEZA AUTOMOTRIZ

Oficio: ELÉCTRICOS

Descripción: INSTALACIONES ELECTRICAS BAJO Y MEDIO

Experiencia:

2023/01/03

SOPORTE TECNICO /

* REALIZACIÓN DE MANTENIMIENTO PREVENTIVO Y CORRECTIVO EN IMPRESORAS PARA LA EMISIÓN DE CÉDULAS Y PASAPORTES A NIVEL NACIONAL Y EN EL EXTRANJERO.
* ATENCIÓN DE REQUERIMIENTOS DE SOPORTE TÉCNICO EN LA MESA DE SERVICIO CUMPLIENDO TURNOS ROTATIVOS.

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, RD

- COORDINACIÓN Y SUPERVISIÓN EFECTIVA DEL EQUIPO TECNOLÓGICO, DIRIGIENDO INICIATIVAS ESTRATÉGICAS Y OPTIMIZANDO RECURSOS PARA LOGRAR LOS OBJETIVOS DEL DEPARTAMENTO.

2022/11/01 **2022/12/31**

CENSISTA / INSTITUTO NACIONAL DE ESTADISTICA Y CENSOS

- GESTIÓN Y SINCRONIZACIÓN PRECISA DE INFORMACIÓN CON PLATAFORMAS DIGITALES
- RECOPILACIÓN DE DATOS CENSALES EN ENTORNOS DE CAMPO

2020/02/10 **2020/10/28**

ASISTENTE DE INGENIERIA / EMELNORTE

- REALIZACIÓN DEL MAPEO DE SEÑALES ANALÓGICAS MEDIANTE EL PROTOCOLO DNP3 EN MEDIDORES DE ENERGÍA ELÉCTRICA (ION), ASÍ COMO LA INTEGRACIÓN EFECTIVA DE DATOS AL CENTRO NACIONAL DE CONTROL DE ENERGÍA (CENACE).
- REALIZACIÓN DE ANÁLISIS DETALLADO Y CORRECCIÓN DE ERRORES EN LA COMUNICACIÓN REMOTA CON EL CENTRO DE CONTROL SCADA EN SUBESTACIONES ELÉCTRICAS. .
- DISEÑO E IMPLEMENTACIÓN DE CIRCUITOS DE CONTROL INDUSTRIAL PARA LA APERTURA Y CIERRE DE ALIMENTADORES EN SUBESTACIONES ELÉCTRICAS, TANTO DE MANERA LOCAL COMO REMOTA.
- REALIZACIÓN DE PRUEBAS, IDENTIFICACIÓN Y CORRECCIÓN DE ERRORES DE COMUNICACIÓN ENTRE RECONECTADORES TRIFÁSICOS DE CARGA ELÉCTRICA Y EL CONCENTRADOR DE DATOS EN SUBESTACIONES ELÉCTRICAS.
- REVISIÓN Y VERIFICACIÓN DE COTIZACIONES DE BIENES Y SERVICIOS PARA EL SUMINISTRO, INSTALACIÓN Y PUESTA EN MARCHA DE EQUIPOS DESTINADOS A LA AUTOMATIZACIÓN DE SUBESTACIONES ELÉCTRICAS

2015/06/09 **2019/08/08**

ARBITRO CENTRAL / AAAFI

- FACILITAR LA COMUNICACIÓN EFECTIVA Y RESOLVER CONFLICTOS DURANTE EL PARTIDO



- LIDERAZGO EFECTIVO Y GESTIÓN DE EQUIPOS, DEMOSTRANDO HABILIDAD PARA MOTIVAR, GUIAR Y DIRIGIR INDIVIDUOS HACIA EL CUMPLIMIENTO DE METAS Y NORMATIVAS

Idioma:

ESPAÑOL	Nivel Hablado:	NATIVO
	Nivel Escrito:	NATIVO
INGLÉS	Nivel Hablado:	BÁSICO
	Nivel Escrito:	INTERMEDIO

Capacitación:

TALLER (61 horas)

SUPERVISOR DE OPERACIONES

CARLOS SLIM

INGENIERÍA/TÉCNICO

TALLER (30 horas)

EXCEL AVANZADO: FUNCIONES Y MANIPULACION DE DATOS

CENFORPRO

INFORMÁTICA SOFTWARE

DIPLOMADO (20 horas)

AUTOMATIZACION Y PROGRAMACION CON PLC

EDUTIN

INGENIERÍA/TÉCNICO

TALLER (40 horas)

ANALISIS DE REDES ELECTRICAS DE DISTRIBUCION EN ARCGIS

INGENIERÍA/TÉCNICO

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

JORNADA (120 horas)

LEVEL-III TRAINING ON IXLA ID5-20

IXLA

INGENIERÍA/TÉCNICO

Referencias Personales:

WILMAN ESPINOZA DELGADO

0993702818

nespinoza@emelnorte.com

CAROLINA MIÑO JARAMILLO

0996726582

cmonse_1@hotmail.com

CARLOS TRAVEZ

0987351166

ctravez@.net

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

3.1.6 Documentos Técnicos

3.1.6.1 Resumen ejecutivo

TÉCNICO EN CAMPO CON EXPERIENCIA EN LA PRODUCCIÓN DE DOCUMENTOS DE IDENTIDAD NACIONALES MEDIANTE MODELO DESCENTRALIZADO DE IMPRESIÓN,

NIXON PAUL ESPINOZA NOBOA

TÉCNICO EN CAMPO CON EXPERIENCIA EN LA PRODUCCIÓN DE DOCUMENTOS DE IDENTIDAD NACIONALES MEDIANTE MODELO DESCENTRALIZADO DE IMPRESIÓN,	**ROL**	**DETALLE DE LA EXPERIENCIA**
Técnico de campo con experiencia en producción de documentaos de identidad, pasaportes electrónicos, y la provisión de equipamiento, suscripciones-licencias de software, insumos y servicios conexos para la Dirección General de Registro Civil Identificación y cedulación (DIGERCIC)	Servicios de instalación, soporte y mantenimiento a la infraestructura de impresión a nivel nacional y países en el exterior (reparar en Nueva York (los equipos de Estados Unidos y Canadá) y en Madrid (los equipos de Europa).	**Dirección General de Registro Civil, Identificación y Cedulación** Republica de Ecuador  Vigencia: Fecha 2019 a la fecha Técnico de campo para para brindar servicios de instalación, soporte y mantenimiento a la infraestructura de impresión para la producción de documentaos de identidad, pasaportes electrónicos, y la provisión de equipamiento, suscripciones-licencias de software, insumos y servicios conexos en la Republica de Ecuador y en el exterior. Descripción de la contratación: Adquisición, implementación de un sistema informático para la emisión de documentos de identidad y pasaportes electrónicos y provisión de equipos, suscripciones – licencias de software, insumos y servicios conexos para la Dirección General de Registro Civil, Identificación y cedulación (DIGERCIC).

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

		Sistema para la emisión de documentos de identidad personal (cedula) de policarbonato y pasaportes electrónicos, PKI/ National PKD/ICAO PKD, ABIS Infraestructura de centro de datos principal y secundario, equipamiento para agencias de atención a nivel nacional y en consulados de Ecuador, para un total de 183 agencias de atención nacional para DIGERCIC y 25 agencias de Ministerio de Relaciones Exteriores y Movilidad Humana (MREMH). Descripción detallada del proyecto: Suministro, instalación y configuración de un sistema Web descentralizado para el enrolamiento Personalización y emisión de documentos de identidad Personal en Policarbonato (100%) formato ID1 y pasaportes electrónicos (EPass) formato ID3 Sistema de inspección biométrico automatizado de huellas y rostro (ABIS) para 16 millones de registros. Sistema de servicios web para búsqueda 1 a 1 y 1 a N de huellas y rostros integrado al ABIS. Capacidad mínima de 10 mil a 20 mil búsquedas diarias Infraestructura de llave pública (PKI) y su integración y conexión al Directorio de claves públicas de la OACI, se incluyeron módulos de seguridad (HSM) para el resguardo de llaves Suministro de infraestructura (HW), licencias, suscripciones de software necesarias para la

EMDOC
Santo Domingo, R.D.

		implementación de un centro de datos primario en alta disponibilidad y un sitio secundario para la recuperación de desastres. Suministro de kits – equipos de captura biométrica, producción y entrega de documentos, ambos en esquema descentralizado. Se incluyo como parte del proyecto la capacitación, transferencia de conocimientos, instalación, configuración, puesta en operación, pruebas unitarias y de integración de los sistemas centrales. Migración de la base de datos biométrica de más de 13.9 millones de registro. Este contrato incluyo el enrolamiento, personalización y emisión de pasaportes electrónicos en 25 agencias nacionales en Ecuador y 3 externas (Consulado de New York, Madrid y una oficina en Quito). Este contrato también incluyo la emisión en el Ecuador de cedulas de identidad personal en policarbonato en 183 agencias de acuerdo con los lineamientos de la OACI 9303. De igual forma incluyo servicios de post implementación, los cuales abarcan soporte técnico, mantenimiento preventivo y correctivo con niveles de servicio de 24x7x365 para todos los componentes del sistema. Importante señalar que como parte de un contrato complementario se contrató una solución de identidad digital y firma electrónica para la ciudadanía.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

		Manejar y configurar impresoras y dispositivos de hardware.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

536

ING. PABLO ROBERTO IBARRA

6749-3355 / 6553-5150

Objetivo:

Formar parte de esta prestigiosa y sólida empresa/ entidad y juntos desarrollar al máximo mi capacidad potencial, para el logro de nuestras metas y la adquisición de nuevos conocimientos en mi campo profesional.

Datos Personales

- **Nacionalidad:** panameña - Estado **Civil:** Unido - **Cédula:** 8-802-1672
  Fecha de Nacimiento: 14/12/1983 - **Edad:** 39 años

Formación Académica

- **Maestría en Gerencia y Transporte Multimodal** /Universidad Interamericana de Panamá (UIP) / 2017.
- **Postgrado en Gerencia/** Universidad Interamericana de Panamá (UIP) / 2016
- **Licenciatura en Ingeniería Industrial** /Universidad Latinoamericana de Ciencia y Tecnología (ULACIT)
- **Bachiller en Letras/** Escuela Americana.
- **Certificado de Sexto Grado/** Escuela Amelia Denis de Icaza.

Cursos, Congresos y Seminarios:

- Curso de Logística
- Curso para Maestro de Teología
- Curso de Manejo de Bodega y de inventario
- Curso de conocimiento de las normas ISO 9001 del 2015 y 2009.
- Curso de auditor de la norma ISO 9001 del 2015 y 2009
- Curso de primeros auxilios
- Curso de manejo de extintores

Conocimiento y Habilidades

- **Gestión de Empresas y de Procesos:** Planificación Estratégica, conocimientos de administración, auditoria, control de inventarios, Procesos y Logística.
- **Informática:** Manejo Avanzado de Office (Word, Excel, Power Point, sap, wms, Barco Box e Internet.

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo

Experiencia **Profesional**

2015- Actualidad: GSI International INC.

Cargo: **Coordinador de Logística y soporte**

Funciones: Coordinar toda la logística de la empresa, desde entrega, pedidos, inventario de tarjeta de documentos seguros, mejoras a procesos, estimados de tiempo de entregas, instalaciones en las sucursales a nivel nacional. Coordinación a nivel nacional en todas las sucursales.

Formé parte del Proyecto de pasaporte electrónico de Ecuador y documento de identidad personal dando el servicio técnico para la solución en:

- **Manejo y configuración de impresora y dispositivos de hardware**

- **Forme parte del Proyecto de cédula de identidad personal de Panamá en:**
  - **Manejo y configuración de impresora y dispositivos de hardware**

2014 - 2015 : Barraza, S.A.

Cargo: **Asistente de Gerente de Logística**

Funciones: Coordinar la entrega de materiales en la planta a centro de distribución. Control de Inventario de materia prima.

2013 - 2014 : Conway Store

Cargo: **Auditor de Control de Inventario**

Funciones: Verificar el cumplimiento de los procesos de la empresa, mediante el control de inventario físicamente de manera continua, con el objeto que se cumpla con lo establecido en las normas de procedimiento de inventario. Luego Encargado de centro de registro:
Donde me encargaba de planificar las actividades de la bodega.

2009 - 2013 : Achura Systens / Chile

Cargo: **Supervisor de Área**

Funciones: Encargado de las coordenadas, medidas, puntos concernientes a la agrimensura; fabricaba perfiles, estructuras, entre otras. De igual manera supervisar al personal, verificar la calidad del trabajo, la seguridad de los trabajadores, a fin de que cuenten con todas las medidas de seguridad y velar con que se cumpla con la producción establecida.

2009 : Escuela El Buen Pastor

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo R.D.

Cargo: **Profesor de Matemáticas**

Funciones: Dictar clases de matemáticas a alumnos de VII, IX, X y XII.

2007 - 2008 : Achura Systens / Panamá

Cargo: **Jefe de Bodega y Supervisor de Área**

Funciones: Recibir los embarques de mercancía, almacenamiento, inventario, pedidos, organización y custodia en la bodega y coordinar las entregas del citado material; de igual manera supervisar al personal, verificar la calidad del trabajo, la seguridad de los trabajadores, a fin de que cuenten con todas las medidas de seguridad y velar con que se cumpla con la producción establecida.

Referencias Personales

- **Licda. María Milagros Velásquez – Abogada-** / Cel. 6775-4396
- **Lcdo. Yuleika Rivas – Contadora** / Cel. 6150-5040

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

3.1.6 Documentos Técnicos

3.1.6.1 Resumen ejecutivo

TÉCNICO EN CAMPO CON EXPERIENCIA EN LA PRODUCCIÓN DE DOCUMENTOS DE IDENTIDAD NACIONALES MEDIANTE MODELO DESCENTRALIZADO DE IMPRESIÓN.

PABLO IBARRA

TÉCNICO EN CAMPO CON EXPERIENCIA EN LA PRODUCCIÓN DE DOCUMENTOS DE IDENTIDAD NACIONALES MEDIANTE MODELO DESCENTRALIZADO DE IMPRESIÓN,	**DESCRIPCION DEL ROL**	**DETALLE DE LA EXPERIENCIA**
Técnico de campo para brindar los Servicios de instalación, soporte y mantenimiento a la infraestructura de impresión a nivel nacional y países en el exterior (en Nueva York (los equipos de Estados Unidos y Canadá) y en Madrid (los equipos de Europa).	Servicios de instalación, soporte y mantenimiento a la infraestructura de impresión a nivel nacional y países en el exterior (reparar en Nueva York (los equipos de Estados Unidos y Canadá) y en Madrid (los equipos de Europa).	Dirección General de Registro Civil, Identificación y Cedulación Republica de Ecuador Vigencia: Fecha 2019 a la fecha Técnico de campo para para brindar servicios de instalación, soporte y mantenimiento a la infraestructura de impresión para la producción de documentaos de identidad, pasaportes electrónicos, y la provisión de equipamiento, suscripciones-licencias de software, insumos y servicios conexos en la Republica de Ecuador y en el exterior. Descripción de la contratación: Adquisición, implementación de un sistema informático para la emisión de documentos de identidad y pasaportes electrónicos y provisión de equipos, suscripciones – licencias de software, insumos y servicios conexos para la Dirección General de Registro Civil, Identificación y cedulación (DIGERCIC).

EMDOC CONSORCIO Santo Domingo, RD

		Sistema para la emisión de documentos de identidad personal (cedula) de policarbonato y pasaportes electrónicos, PKI/ National PKD/ICAO PKD, ABIS Infraestructura de centro de datos principal y secundario, equipamiento para agencias de atención a nivel nacional y en consulados de Ecuador, para un total de 183 agencias de atención nacional para DIGERCIC y 25 agencias de Ministerio de Relaciones Exteriores y Movilidad Humana (MREMH). Descripción detallada del proyecto: Suministro, instalación y configuración de un sistema Web descentralizado para el enrolamiento Personalización y emisión de documentos de identidad Personal en Policarbonato (100%) formato ID1 y pasaportes electrónicos (EPass) formato ID3 Sistema de inspección biométrico automatizado de huellas y rostro (ABIS) para 16 millones de registros. Sistema de servicios web para búsqueda 1 a 1 y 1 a N de huellas y rostros integrado al ABIS. Capacidad mínima de 10 mil a 20 mil búsquedas diarias Infraestructura de llave pública (PKI) y su integración y conexión al Directorio de claves públicas de la OACI, se incluyen módulos de seguridad (HSM) para el resguardo de llaves. Suministro de infraestructura (HW), licencias, suscripciones de

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

		software necesarias para la implementación de un centro de datos primario en alta disponibilidad y un sitio secundario para la recuperación de desastres. Suministro de kits – equipos de captura biométrica, producción y entrega de documentos, ambos en esquema descentralizado. Se incluyo como parte del proyecto la capacitación, transferencia de conocimientos, instalación, configuración, puesta en operación, pruebas unitarias y de integración de los sistemas centrales. Migración de la base de datos biométrica de más de 13.9 millones de registro. Este contrato incluyo el enrolamiento, personalización y emisión de pasaportes electrónicos en 25 agencias nacionales en Ecuador y 3 externas (Consulado de New York, Madrid y una oficina en Quito). Este contrato también incluyo la emisión en el Ecuador de cedulas de identidad personal en policarbonato en 183 agencias de acuerdo con los lineamientos de la OACI 9303. De igual forma incluyo servicios de post implementación, los cuales abarcan soporte técnico, mantenimiento preventivo y correctivo con niveles de servicio de 24x7x365 para todos los componentes del sistema. Importante señalar que como parte de un contrato complementario se contrato una solución de identidad digital y

CONSORCIO EMDOC
CONSORCIO
Santo Domingo, RD

		firma electrónica para la ciudadanía. Manejar y configurar impresoras y dispositivos de hardware.
		TRIBUNAL ELECTORAL DE PANAMA FABRICA DE DOCUMENTO DE IDENTIDAD PERSONAL (Cédula) +SISTEMA BIOMETRICO DE IDENTIFICACION CIUDADANA (ABIS): Año 2016 hasta año 2022 República de Panamá: Técnico responsable del soporte a nivel nacional y en el extranjero, con experiencia en la producción de documentos de identidad nacional, incluyendo el soporte de equipos tecnológicos y las impresoras. Descripción del proyecto Solución de impresión para el documento de identidad personal panameño (Cédula). Contrato N0.24/2016/DS Provisión, Desarrollo de Sistemas tales como Sistema de Gestor de Hardware, gestor de producción, gestor de inventarios, distribución, reportes, entre otros (Impresora de documento de identidad personal) y Suministros de 4,500,000 tarjetas (Documento de Identidad Personal) equipamiento tecnológico, aplicativo, insumos y servicio de mantenimiento y soporte para el centro de

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

		impresión de documento de identidad personal del Tribunal Electoral de Panamá. Valor aproximado del contrato $.6,519,565.42 seis millones quinientos diecinueve mil, quinientos sesenta y cinco con 42/100 dólares de los Estados Unidos de América. ABIS: Numero de registros soportado el sistema ABIS El volumen es de (10,000,000) diez millones de registros (personas) Suministro, instalación y soporte, mantenimiento y actualización del sistema biométrico de identificación ciudadana (ABIS), para la extracción, conversión y migración de todos los datos del sistema actual a la nueva solución para ser utilizada en la Dirección de Tecnología de la Información y comunicación (DTIC) del Tribunal Electoral de Panamá. Contrato de soporte y mantenimiento para el sistema impresión/emisión.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

9

544

RAÚL ALEXIS CUELLO VICENTE

829 604 3255 | ing.raulc@hotmail.com | Santo Domingo D. N.

EXPERIENCIA

Líder Desarrollo (9/2022-Actual)

Ing. Especialista en Aplicaciones (10/2021)

GSI INTERNACIONAL

10/2021 – Actual | República Dominicana

- Desarrollo y customización aplicaciones comerciales.
- Automatizaciones de procesos.
- Desarrollo y consumo de servicios de aplicaciones API y Web Services.
- Gestión Documental

Analista Programador

FONT GAMUNDI, S. A.

12/2016 – 10/21 | República Dominicana

- Responsable de la calidad del desarrollo del sistema y el empaquetado del mismo, asegurando que se cumplan las políticas de desarrollo tanto técnicas como administrativas.
- Gestión de cambios sugeridos por clientes internos y externos para el sistema.
- Encargado del entrenamiento a nuevos miembros del equipo de desarrollo.
- Desarrollo, soporte e integración de interfaces para el ERP de la empresa. Destacando: Sistemas de almacenamiento y distribución, Ventas móviles e Integraciones con sistemas externos (Clientes Externos).

Tec. Ejecutivo Internacional

CSQ Dominicana

01/2016 - 11/2016 | República Dominicana

- Soporte y gestión a cliente interno y externos.
- Gestión de configuración del API RESTfull.
- Programación con C# y SQL Server.
- Configuración de los distintos protocolo de enrutamiento entre clientes y proveedores y operadores de recargas

EDUCACIÓN

Ingeniero de Sistemas Y Computación

Universidad Dominicana O&M

Maestría

Master Executive MBA Dirección Estratégica

Escuela de Negocios Formato Educativo (España) y Universidad de Cádiz (Colombia)

OTROS ESTUDIOS

.

- BIZAGI Certified Professional Associate
- SCRUM Fundamentos
- Emprendedor para Pymes
- Back End Asp.net y SQL Server
- ITIL V3
- Liderazgo y Supervisión
- Locución
- Servicio al Cliente
- Protección de datos
- Plan de Negocios
- ASP.NET MVC avanzado
- Ingles de Inmersión
- Manejo Efectivo del Tiempo
- Maestro de Ceremonias
- Supervisión Efectiva

IDIOMAS

Español
Nativo

Ingles
Avanzado

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

4

3.1.6 Documentos Técnicos

3.1.6.1 Resumen ejecutivo

TÉCNICO EN CAMPO CON EXPERIENCIA EN LA PRODUCCIÓN DE DOCUMENTOS DE IDENTIDAD NACIONALES MEDIANTE MODELO DESCENTRALIZADO DE IMPRESIÓN.

RAUL ALEXIS CUELLO VICENTE

TÉCNICO EN CAMPO CON EXPERIENCIA EN LA PRODUCCIÓN DE DOCUMENTOS DE IDENTIDAD NACIONALES MEDIANTE MODELO DESCENTRALIZADO DE IMPRESIÓN,	DESCRIPCION DEL ROL	DETALLE DE LA EXPERIENCIA
Técnico de campo para brindar los Servicios de instalación, soporte y mantenimiento a la infraestructura de impresión a nivel nacional y países en el exterior (en Nueva York (los equipos de Estados Unidos y Canadá) y en Madrid (los equipos de Europa).	Servicios de instalación, soporte y mantenimiento a la infraestructura de impresión a nivel nacional y países en el exterior (reparar en Nueva York (los equipos de Estados Unidos y Canadá) y en Madrid (los equipos de Europa).	**Dirección General de Registro Civil, Identificación y Cedulación** **Republica de Ecuador**  Vigencia: Fecha 2019 a la fecha Técnico de campo para para brindar servicios de instalación, soporte y mantenimiento a la infraestructura de impresión para la **producción de documentaos de identidad, pasaportes electrónicos, y la provisión de equipamiento, suscripciones-licencias de software, insumos y servicios conexos en la Republica de Ecuador y en el exterior.** Descripción de la contratación: Adquisición, implementación de un sistema informático para la emisión de documentos de identidad y pasaportes electrónicos y provisión de equipos, suscripciones – licencias de software, insumos y servicios conexos para la Dirección General de Registro Civil, Identificación y cedulación (DIGERCIC). Sistema para la emisión de documentos de identidad personal (cedula) de policarbonato y pasaportes electrónicos, PKI/ National PKD/ICAO PKD, ABIS **Infraestructura de centro de datos principal y secundario, equipamiento para agencias de atención a nivel nacional y en consulados de Ecuador, para un total de 183 agencias de atención nacional para DIGERCIC y 25 agencias de Ministerio de Relaciones Exteriores y Movilidad Humana (MREMH).** Descripción detallada del proyecto: Suministro, instalación y configuración de un sistema Web descentralizado para el enrolamiento

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

		formato ID1 y pasaportes electrónicos (EPass) formato ID3 Sistema de inspección biométrico automatizado de huellas y rostro (ABIS) para 16 millones de registros. Sistema de servicios web para búsqueda 1 a 1 y 1 a N de huellas y rostros integrado al ABIS. Capacidad mínima de 10 mil a 20 mil búsquedas diarias Infraestructura de llave pública (PKI) y su integración y conexión al Directorio de claves públicas de la OACI, se incluyeron módulos de seguridad (HSM) para el resguardo de llaves. Suministro de infraestructura (HW), licencias, suscripciones de software necesarias para la implementación de un centro de datos primario en alta disponibilidad y un sitio secundario para la recuperación de desastres. Suministro de kits – equipos de captura biométrica, producción y entrega de documentos, ambos en esquema descentralizado. Se incluyo como parte del proyecto la capacitación, transferencia de conocimientos, instalación, configuración, puesta en operación, pruebas unitarias y de integración de los sistemas centrales. Migración de la base de datos biométrica de más de 13.9 millones de registro. Este contrato incluyo el enrolamiento, personalización y emisión de pasaportes electrónicos en 25 agencias nacionales en Ecuador y 3 externas (Consulado de New York, Madrid y una oficina en Quito). Este contrato también incluyo la emisión en el Ecuador de cedulas de identidad personal en policarbonato en 183 agencias de acuerdo con los lineamientos de la OACI 9303. De igual forma incluyo servicios de post implementación, los cuales abarcan soporte técnico, mantenimiento preventivo y correctivo con niveles de servicio de 24x7x365 para todos los componentes del sistema. Importante señalar que como parte de un contrato complementario se contrató una solución de identidad digital y firma electrónica para la ciudadanía. Manejar y configurar impresoras y dispositivos de hardware.
		TRIBUNAL ELECTORAL DE PANAMA

CONSORCIO EMDOC CONSORCIO Santo Domingo, R

		FABRICA DE DOCUMENTO DE IDENTIDAD PERSONAL (Cédula) +SISTEMA BIOMETRICO DE IDENTIFICACION CIUDADANA (ABIS): Año 2016 hasta año 2022 República de Panamá:  Técnico responsable del soporte a nivel nacional y en el extranjero, con experiencia en la producción de documentos de identidad nacional, incluyendo el soporte de equipos tecnológicos y las impresoras. Descripción del proyecto Solución de impresión para el documento de identidad personal panameño (Cédula). Contrato NO.24/2016/DS Provisión, Desarrollo de Sistemas tales como Sistema de Gestor de Hardware, gestor de producción, gestor de inventarios, distribución, reportes, entre otros (Impresora de documento de identidad personal) y Suministros de 4,500,000 tarjetas (Documento de Identidad Personal) equipamiento tecnológico, aplicativo, insumos y servicio de mantenimiento y soporte para el centro de impresión de documento de identidad personal del Tribunal Electoral de Panamá. Valor aproximado del contrato $.6,519,565.42 seis millones quinientos diecinueve mil, quinientos sesenta y cinco con 42/100 dólares de los Estados Unidos de América. ABIS: Numero de registros soportado el sistema ABIS El volumen es de (10,000,000) diez millones de registros (personas) Suministro, instalación y soporte, mantenimiento y actualización del sistema biométrico de identificación ciudadana (ABIS), para la extracción, conversión y migración de todos los datos del sistema actual a la nueva solución para ser utilizada en la Dirección de Tecnología de la Información y comunicación (DTIC) del Tribunal Electoral de Panamá. Contrato de soporte y mantenimiento para el sistema impresión/emisión.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

548

ALEX GEOVANNY BARRAGÁN LLANOS



Datos Personales

Dirección:	FELIZA EGUEZ #107 y CONVENCION DE 1884
Teléfono (s):	551943 - 0994021941 - 0999495987 -
Cédula de identidad:	0202047726
Correo electrónico:	alexbarragan_@hotmail.com
Ciudad / Provincia / País:	GUARANDA / BOLIVAR / ECUADOR

Instrucción Formal

MAGISTER EN GESTION TECNOLOGICA — CUARTO NIVEL - MAESTRIA

(1 AÑOS) UNIVERSIDAD INTERNACIONAL DE LA RIOJA

INGENIERO EN SISTEMAS COMPUTACIONALES — TERCER NIVEL

(5 AÑOS) UNIVERSIDAD ESTATAL DE BOLIVAR

BACHILLER CIENCIAS FÍSICO MATEMÁTICO — BACHILLER

(6) UNIDAD EDUCATIVA VERBO DIVINO

BACHILLER EN TÉCNICO EN COMERCIO Y ADMINISTRACIÓN INFORMÁTICA — BACHILLER

(6) UNIDAD EDUCATIVA PCEI INTERNACIONAL BOLIVAR

CONSORCIO EMDOC
EMDOC CONSORCIO
Santo Domingo, RD

PRIMARIA /BÁSICA ELEMENTAL

Experiencia:

1/10/2024

GSI INT. INC. – Actualidad

PERSONAL TECNICO DE CAMPO:

Experiencia en la producción de documentos de identidad nacionales, experiencia en impresión, servicios de instalación, soporte y mantenimiento a la infraestructura de impresión y producción de documentos de identidad nacional.

2023/09/18

DOCENTE / UNIDAD EDUCATIVA GARCIA

* DOCENTE DEL AREA DE TECNOLOGIAS DE LA INFORMACION, TUTOR DE TERCER AÑO DE BACHILLERATO Y DIRECTOR DE PRACTICAS PREPROFESIONALES

2022/08/15 2023/06/26

DOCENTE / UNIDAD EDUCATIVA SANTA MARIANA DE JESUS

* DOCENTE DEL AREA DE INFORMATICA, TUTOR DE DECIMO AÑO DE BACHILLERATO, DIRIGENTE DEL GRUPO DE PROGRAMACION EN NIÑOS.

2021/07/07 2022/07/30

TECNICO / WORLDTEC

* INSTALACION DE EQUIPOS DE SEGURIDAD ELECTRONICA Y DOMOTICA

2019/04/24 2021/06/01

TECNICO / SEGURIDAD Y TECNOLOGIA DEL ECUADOR CIA.LTDA

* INTALACION DE EQUIPOS DE DOMOTICA, SEGURIDAD ELECTRONICA Y REDES DE COMPUTADORAS.

2016/09/05

DOCENTE / UNIDAD EDUCATIVA PCEI INTERNACIONAL BOLIVAR

* SEGUIMIENTO Y CONTROL DE ACTIVIDADES DE ESTUDIANTES, CONTROL DE CONDUCTA Y DISCIPLINA, OORDINACION DE ATIVIDADES CON PADRES DE FAMILIA
* CONTROL DEL PERSONAL DOCENTE ADMINISTRATIVO Y DE SERVICIO, COORDINACION DE ACTIVIDADES INHERENTES A LA UNIDAD EDUCATIVA.

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

Idioma:

INGLÉS	Nivel Hablado:	INTERMEDIO
	Nivel Escrito:	INTERMEDIO

Capacitación:

SEMINARIO	**CURSO DE MEGA PROYECTOS EN SEGURIDAD ELECTRÓNICA**
(40 horas)	**CENTRO DE CAPACITACIÓN ECUADOR**
	INFORMÁTICA/TELECOMUNICACIONES
JORNADA	**INTRODUCCIÓN A INTERNET DE TODO**
(8 horas)	**CISCO NETWORKING ACADEMY**
	INFORMÁTICA/TELECOMUNICACIONES
SEMINARIO	**CONTINUING EDUCATION CERTIFICATE IN LEADERSHIP**



(45 horas)

MARCONI INTERNATIONAL UNIVERSITY

ADMINISTRACIÓN/OFICINA

TALLER **FORMACIÓN DE FORMADORES - METODOLOGÍA INAP**

(60 horas) **SECAP**

EDUCACIÓN BÁSICA/CURSOS

CONSORCIO EMDOC
EMDOC CONSORCIO
Santo Domingo, R.D.

552

Acciones Afirmativas

Nota: Las acciones afirmativas se sumarán, únicamente, a aquellos postulantes que cumplan con los requisitos para recibirlos y siempre que hubieran obtenido la calificación mínima del setenta por ciento (70%) en el puntaje de

Autodeterminación étnica:	MESTIZO/A
Discapacidad:	NO
Enfermedad catastrófica:	NO
A cargo de familiar con	NO
A cargo de familiar con	NO
Migrante Ex-Servidor Público:	NO
Residente provincia de	NO
Residente Amazónico:	NO

Referencias Personales

FANNY GABRIELA BARRAGAN QUISHPE

0958764725

ROSARIO DIOCELINA LOPEZ

0981157072

CESAR AUGUSTO SALTOS BAECILLA

0994155477

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

9

553

LA REPÚBLICA DEL ECUADOR

En su nombre y por autoridad de la ley,

LA UNIVERSIDAD ESTATAL DE BOLÍVAR

Por medio de la Facultad de Ciencias Administrativas,
Gestión Empresarial e Informática

Considerando que:

BARRAGAN LLANOS ALEX GEOVANNY

Ha cumplido con los requisitos de Ley, Estatuto y Reglamentos, le confiere el TÍTULO de:

INGENIERO EN SISTEMAS COMPUTACIONALES

Por el cual se le reconocerán y guardarán sus derechos, honores y privilegios que le corresponden de conformidad con la Ley.

Dado y firmado en la ciudad de Guaranda a los **Dieciséis** días del mes de **Octubre** del año 2020

UNIVERSIDAD ESTATAL DE BOLÍVAR SECTORADO

Dr. C. ARTURO ROJAS S.
RECTOR

Ing. MÓNICA BONILLA M.
DECANO

Abg. MÓNICA LEÓN G.
SECRETARIO GENERAL

Universidad Estatal de Bolívar Secretaría General

FCAGEI N° 0002451

Registrado y refrendado en el Libro de Grados y Títulos respectivo con el No. 94366
en el folio 2394 24-11 del 20 20
Cc.: 0202047726

FCAGEI0002451

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

UNIVERSIDAD ESTATAL DE BOLÍVAR

Felipe VI, Rey de España

y en su nombre

el Rector de la Universidad Internacional de La Rioja

unir
UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Considerando que, conforme a las disposiciones y circunstancias previstas por la legislación vigente,

Don Alex Geovanny Barragán Llanos

nacido el 29 de enero de 1993 en Guaranda (Ecuador), de nacionalidad ecuatoriana,
ha superado en noviembre de 2021, los estudios conducentes al TÍTULO oficial de

Máster Universitario en Dirección y Gestión de Tecnologías de la Información (TI) por la Universidad Internacional de La Rioja

establecido por Acuerdo del Consejo de Ministros de 1 de septiembre de 2020,
expide el presente título oficial con validez en todo el territorio nacional,
que faculta al interesado para disfrutar los derechos que a este título
otorgan las disposiciones vigentes.

Dado en Logroño, a 22 de diciembre de 2021

El interesado,

Alex Geovanny Barragán Llanos

El Rector,

José María Vázquez García-Peñuela

La Jefa del Departamento de Títulos,

Laura Herrera Navarro

Código de Universidad	Registro Nacional de Títulos	Código de Centro	Registro Universitario de Títulos
877	1021394691	26004787	80295

UNIR A-26004787

CONSORCIO EMUDOC

R.D. 1027/2011

GOBIERNO DE LA REPÚBLICA DEL ECUADOR

MINISTERIO DE EDUCACIÓN

EN SU NOMBRE Y POR AUTORIDAD DE LA LEY LA INSTITUCIÓN EDUCATIVA

UNIDAD EDUCATIVA VERBO DIVINO

CONFIERE A:

BARRAGAN LLANOS ALEX GEOVANNY

EL TÍTULO DE BACHILLER

CIENCIAS

FÍSICO MATEMÁTICAS

Por haber aprobado los estudios reglamentarios en el nivel de Bachillerato,
con la calificación de **16.00 (DIECISEIS COMA CERO)**

Dado y firmado en: **BOLIVAR, 02 de julio de 2010**

MGS. ARGUELLO ESTRELLA TERESITA LOURDES
Rector (a)

LIC. DAVILA ALVAREZ CARMEN BEATRIZ
Secretario(a)

UNIDAD EDUCATIVA VERBO DIVINO
SECRETARÍA
GUARANDA

UNIDAD EDUCATIVA FISCOMISIONAL
VERBO DIVINO
RECTOR

CONSORCIO ECUATORIANO
Domingo

EL GOBIERNO DE TODOS

955

GOBIERNO DE LA REPÚBLICA DEL ECUADOR

MINISTERIO DE EDUCACIÓN

EN SU NOMBRE Y POR AUTORIDAD DE LA LEY LA INSTITUCIÓN EDUCATIVA

INTERNACIONAL BOLIVAR

CONFIERE A:

BARRAGAN LLANOS ALEX GEOVANNY

EL TÍTULO DE BACHILLER

TECNICO EN COMERCIO Y ADMINISTRACION INFORMATICA

Por haber aprobado los estudios reglamentarios en el nivel de Bachillerato, con la calificación de **18.00 (DIECIOCHO COMA CERO)**

Dado y firmado en: **CHIMBORAZO, 26 de septiembre de 2009**

CESAR AUGUSTO SALTOS BAECILLA
Rector (a)

MARIA DE LOURDES LLANOS FIERRO
Secretario(a)

CONSORCIO EMDOC Santo Domingo, RO

956

557

Guaranda, 01 de marzo de 2024

HNA. JUANA DEL ROCÍO MORÁN ROSADO, con cédula de identidad N° **1203809601,** Rectora de la Unidad Educativa "Santa Mariana de Jesús", de la ciudad de Guaranda.

CERTIFICO

Que el señor Ingeniero **ALEX GEOVANNY BARRAGÁN LLANOS,** portador de la cédula de identidad N° 0202047726, laboró en la Unidad Educativa, como docente de la materia de informática, desde el 15 de agosto de 2022 hasta el 26 de junio de 2023.

Es todo cuanto puedo certificar en honor a la verdad, facultando al interesado hacer uso del presente documento en lo que a bien tuviere.

Hna. Juana Morán R., r.m.s
RECTORA

UNIDAD EDUCATIVA "SANTA MARIANA DE JESÚS" RECTORADO GUARANDA

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, RO

558

Guaranda, 17 de agosto del 2022

CERTIFICADO LABORAL

Ing. **Carlos Xavier Poaquiza** con número de cédula N° **0202146718**, en su rol de Gerente propietario de la empresa **"WorldTec"** con RUC **0202146718001** Ubicado en la ciudad de Guaranda, Calle Sucre y Manuela Cañizares.

CERTIFICA:

Que, el Ing. **ALEX GEOVANNY BARRAGAN LLANOS** con número de cédula **N°0202047726,** ha laborado en nuestra empresa como **Soporte Técnico de computadoras, Redes Informáticas y manejo de aplicaciones Ofimáticas.** durante el periodo comprendido desde **07/07/2021** hasta **30 /07/2022**.
Durante su tiempo en la empresa ha demostrado responsabilidad, honestidad y dedicación en las labores que le fueron encomendadas.

Se expide la presente a solicitud del interesado, para los fines que crea conveniente.

Atte.

Ing. Carlos Poaquiza
Gerente propietario
C.I 0202146718
Cel. 0981942369

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

559

UNIDAD EDUCATIVA PCEI
"INTERNACIONAL BOLIVAR"
ACUERDO MINISTERIAL No 326
CODIGO AMIE 02H00812

EL LCDO.CESAR AUGUSTO SALTOS BAECILLA. RECTOR DE LA UNIDAD EDUCATIVA PCEI "INTERNACIONAL BOLÍVAR"

A PETICIÓN VERBAL DE PARTE INTERESADA:

CERTIFICA:

Que el Ing. ALEX GEOVANNY BARRAGAN LLANOS C.I.020204772-6, trabajó en nuestra institución como docente en el área de informática en el ciclo de básica superior y bachillerato, en el periodo lectivo 2016-2017- 2017-2018 -2018-2019 2019-2020-2020-2021 y 2021-2022, demostrando responsabilidad y esmero en todas las tareas encomendadas a él, haciéndose acreedora de nuestra estima y consideración.

Es todo cuanto puedo certificar en honor a la verdad, autorizando al interesado dar al presente el uso que creyere conveniente a su interés.

Guaranda, Agosto 02 de 2022

Atentamente

I.CDO. AUGUSTO SALTOS B.
RECTOR
RUC: 0200569952001

UNIDAD EDUCATIVA PARTICULAR A DISTANCIA INTERNACIONAL BOLIVAR GUARANDA RECTORADO

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

Calidad y excelencia en Educación a Distancia...
Dirección: Avda 5 de Junio Telf.: 032 553 061
E mail saltosbaecilla@hotmail.com
Guaranda – Ecuador

560

SEGURIDAD Y TECNOLOGIA DEL ECUADOR CIA. LTDA.

Abogado: FABIAN ALEGRIA, GERENTE GENERAL DE "SEGURIDAD Y TECNOLOGIA DEL ECUADOR CIA. LTDA."; a petición de parte interesada:

C E R T I F I C A:

Que el Ing.: ALEX GEOVANNY BARRAGAN LLANOS, portador de la cédula de identidad # 020204772-6, revisados los archivos que reposan en esta Empresa, prestó sus servicios en el Área de TECNOLOGÍA (Ofimática, Domótica, Redes Informáticas) desde el 24 de abril del 2019 hasta el 1 de Junio de 2021, desempeñando sus funciones con total responsabilidad

Es todo cuanto puedo certificar en honor a la verdad, facultando al peticionario hacer uso del presente para los fines legales que creyere conveniente.

EXPEDIDO EN: Guaranda, 27 de julio de 2022

Abg. Fabián Alegría
GERENTE GENERAL "SYTEDEC CIA. LTDA."

SEGURIDAD Y TECNOLOGIA DEL ECUADOR SYTEDEC CIA. LTDA.
RUC: 0291523714001

DIR: CDLA COLONIA ROMAN SUR (GUARANDA – ECUADOR)
TELF: 032552407
CEL: 0998495987
E-MAIL: alegria@yahoo.com

CONSORCIO EMDOC
Santo Domingo, R

000462

Ministerio del Trabajo
Servicio Ecuatoriano de Capacitación Profesional

CERTIFICAN
A

BARRAGAN LLANOS ALEX GEOVANNY

con el número de cédula: 0202047726, habiendo cumplido con los requisitos estipulados en los reglamentos correspondientes, aprobó el curso:

FORMACIÓN DE FORMADORES - METODOLOGÍA INAP

~~En la modalidad VIRTUAL~~ ~~Sector PRODUCTIVO~~

Realizado en GUARANDA del 2022-05-16 al 2022-06-10

Código 85157 Con una duración de 60 HORAS

Dado y firmado en GUARANDA, el 14 de junio de 2022

Director/a Ejecutivo o
Delegado/a del Secap

CONSORCIO EMDOC
EMDOC CONSORCIO
Santo Domingo, R D

República del Ecuador

Gobierno del Encuentro | Juntos lo logramos

Contenido:

- Formulación de metas y objetivos de aprendizaje para la acción formativa.
- Desarrollo de actividades prácticas y evaluaciones para la acción formativa.
- Estrategias metodológicas y programación de las acciones formativas.
- Elaboración de la guía didáctica y ejecución de procesos formativos online, presenciales o mixtos.

Verifique su validez de su certificado, escaneando el gráfico

l usuario del presente certificado descarga y libera al SECAP de toda responsabilidad administrativa, civil o penal que se puedan derivar del uso del ismo. El usuario declara además que es de su exclusiva responsabilidad el uso del presente certificado, siendo el único responsable en la ejecución de s actividades que realice como resultado de la obtención del referido instrumento. De igual forma el usuario, así como sus familiares, herederos o administradores renuncian a instaurar cualquier tipo de demanda o acción legal similar en contra del SECAP, originada en las actividades que trata la certificación. De ser necesario el SECAP se reserva el derecho de investigar y trasladar a las instancias correspondientes las anomalías o novedades.

CONSORCIO EMDOC
EMDOC CONSORCIO
Santo Domingo, R.O.

295



Certificado de finalización

Otorgado a:

Alex Geovanny Barragán Llanos

Nombre

Por haber realizado el curso de Cisco Networking Academy® "Introducción a Internet de todo" y demostrar habilidad para lo siguiente:

- Explicar el impacto, los beneficios y los desafíos de Internet de todo.
- Explicar la interacción entre las personas, los procesos, los datos y las cosas que conforman Internet de todo.
- Explicar cómo las cosas con y sin conexión IP pueden conectarse a una red para comunicarse en el marco de Internet de todo.
- Explicar la creación de modelos y de prototipos en IdT.

Rodrigo Del Pozo

Instructor

05-jun-2018

Fecha

Firma del instructor

CONSORCIO EMDOC, Santo Domingo, R.D.
EMDOC CONSORCIO

563

Cisco Networking Academy®

Mind Wide Open™

Certificado de finalización del curso

CCNA Routing and Switching: Introducción a redes

Durante el curso de Cisco Networking Academy®, impartido por el instructor abajo firmante,el alumno logró desarrollar los siguientes aspectos:

- Explicar las tecnologías de red.
- Explicar cómo los dispositivos tienen acceso a los recursos de red local y remota.
- Describir el hardware del router.
- Explicar la forma en que funciona el switching en una red de pequeña o mediana empresa.
- Diseñar un esquema de direccionamiento IP para proporcionar conectividad de red a una red de una pequeña o mediana empresa.
- Configurar los parámetros iniciales en un dispositivo de red.
- Implementar la conectividad de red básica entre dispositivos.
- Configurar las herramientas de supervisión disponibles para una red de pequeña o mediana empresa.

Alex Geovanny Barragán Llanos
Estudiante

UNIVERSIDAD ESTATAL DE BOLIVAR
Nombre de la academia

Ecuador
Ubicación

07-ago-2018
Fecha

Rodrigo Del Pozo
Instructor

Firma del instructor

CONSORCIO EMDOC, Santo Domingo, R.D.

MARCONI International University | DIVISION OF CONTINUING EDUCATION

Certifies that

Alex Barragán Llanos

Successfully completed the requirements for the

Continuing Education Certificate in Leadership

MIAMI, FL

November 2020 to December 2020 - Hours: 45

Issued on: December 30, 2020

Pablo Cardona
President

MIU

CONSORCIO EMDOC · CONSORCIO EMDOC · SANTO DOMINGO, R.D.

The authenticity of this electronic document can be verified through the following address: https://verisignature.miauniversity.edu/CSV/c70ecb62-4491-42eb-be63-706d299d8a4. Signed by: Pablo Cardona.

Centro de Capacitación Ecuador

otorga el presente

CERTIFICADO

a

Alex Geovanny Barragán Llanos

Curso de Mega Proyectos en Seguridad Electrónica

Realizado en la ciudad de Quito en el mes de Julio de 2019
con una duración de 40 h

Vladyslav Taranchenko
Gerente General

CONSORCIO EMDOC
EMDOC CONSORCIO
Santo Domingo

526

567











CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

568

3.1.6 Documentos Técnicos

3.1.6.1 Resumen ejecutivo

TÉCNICO EN CAMPO CON EXPERIENCIA EN LA PRODUCCIÓN DE DOCUMENTOS DE IDENTIDAD NACIONALES MEDIANTE MODELO DESCENTRALIZADO DE IMPRESIÓN.

Alex Geovanny Barragán Llanos

TÉCNICO EN CAMPO CON EXPERIENCIA EN LA PRODUCCIÓN DE DOCUMENTOS DE IDENTIDAD NACIONALES MEDIANTE MODELO DESCENTRALIZADO DE IMPRESIÓN,	**DESCRIPCION DEL ROL**	**DETALLE DE LA EXPERIENCIA**
Técnico de campo para brindar los Servicios de instalación, soporte y mantenimiento a la infraestructura de impresión a nivel nacional y países en el exterior (en Nueva York (los equipos de Estados Unidos y Canadá) y en Madrid (los equipos de Europa).	Servicios de instalación, soporte y mantenimiento a la infraestructura de impresión a nivel nacional y países en el exterior (reparar en Nueva York (los equipos de Estados Unidos y Canadá) y en Madrid (los equipos de Europa).	Dirección General de Registro Civil, Identificación y Cedulación Republica de Ecuador  Técnico de campo para para brindar servicios de instalación, soporte y mantenimiento a la infraestructura de impresión para la producción de documentaos de identidad, pasaportes electrónicos, y la provisión de equipamiento, suscripciones-licencias de software, insumos y servicios conexos **en la Republica de Ecuador y en el exterior.** 1.Administración y soporte de aplicaciones de hardware y software en el área de cedulación de la DIGERCIC 2.Capacitación y entrenamientos a usuarios de la Digercic 3.Ingeniero experto configuración de equipos especializados. 4.Tareas de mantenimiento correctivo y preventivo en equipos

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

		tecnológicos, impresoras de la fábrica de cedulación en modalidad descentralizada 5.Realizar controles preventivos de funcionalidad, disponibilidad y seguridad. Control del normal funcionamiento del centro de la DIGERCIC 6.Manejar y configurar impresoras y dispositivos de hardware. .

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo

570



Carlos Gomez

CONTACTO

Calle Vieja, El Tablon, 010102, Cuenca, Azuay

0998647446

gomezbonigno8@gmail.com

FORMACIÓN

Tecnólogo en análisis de sistemas: Software
INSTITUTO SUPERIOR SUDAMERICANO - Cuenca, Ecuador, 2016

Bachiller en ciencias básicas: Ciencias comunes Colegio Nacional Benigno Malo - Cuenca, Ecuador, 2011

HISTORIAL LABORAL

Soporte Tecnico
01/2021 - Actual
Soporte técnico de sistema SEDIP e impresoras implamentadas para cedulas y pasaportes.

Ayudante Tecnico Telconet - Cuenca, Azuay
06/2020 - 12/2020
Realizar migraciones de equipos Cisco a ZTE, además tendido de fibra y correcciones de errores encontrados por fiscalización en nodos.

Desarrollador de Software CodeFactory - Cuenca, Azuay
Desarrollador 03/2019 - 08/2019

- de módulos para un CRM, basado en el lenguaje de programación C# y apoyado con base de datos sql server 2014 para institución bancaria.
- Desarrollador de visor geográfico, basado en lenguaje javascript con la librería leaflet

Desarrolladora de Aplicaciones Web Geoinformatica - Cuenca, Azuay
04/2015 - 02/2019 - 09/2019-03/2020

- Programador de proyectos Informáticos
- Programador de proyectos OpenERP
- Programador de proyectos móviles en Apache - Cordova
- Desarrollo de aplicaciones Web
- Dibujante de GIS

APTITUDES

- Gestión de proyectos
- Habilidades multitarea
- Con formación en ArcGis
- Solución de conflictos
- Trabajo en equipo
- Horario flexible
- Interacción con clientes
- Dominio de Ofimática

DIPLOMAS

- PREVENCIÓN DE RIESGOS LABORALES - PREVENCIÓN DE RIESGOS LABORALES: ENERGÍA ELÉCTRICA
- Desarrollador de aplicativos Moviles en Ionic

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

[redacted]

PROYECTOS REALIZADOS

- Empresa / Institución: Dirección General de Registro Civil, Identificación y Cedulación

  Proyecto: Adquisición e implementación de un sistema informático para emisión de documentos de identidad y pasaportes electrónicos, y la provisión de equipamiento, suscripciones-licencias de software, insumos, mantenimiento y servicios conexos para la Dirección General de Registro Civil Identificación y cedulación (DIGERCIC)

  Papel desempeado: Brindar soporte técnico a los equipos de impresión y software a nivel nacional

  Actividades relevantes: Técnico de campo en inspecciones regulares en los equipos de impresión y otros equipos necesarios. Entrenamiento de personal local en el uso y mantenimiento de equipos de impresión y sistemas de codificación, y provisión de soporte técnico para resolver.

- Empresa / Institución: Geoinformatica Consultores
  Contratante: GAD Santiago de Mendez,GAD SALITRE,GAD Otreedo, GAD San Lorenzo, GAD Catamayo
  Proyecto: SISTEMA DE SERVICIOS MUNICIPALES
  Papel desempeñado: Desarrollador de Sistema Informático para el Catastro Urbano y los departamentos del Municipio de el GAD de Méndez en Plataforma OpenERP.
  Tiempo de participación: Abril, 2015-Actualidad
  Actividades relevantes: -Desarrollo de los siguientes Módules del Sistema Municipal:
  -Administración Cartografía (GIS)
  -Emisión de Títulos de Crédito Impuesto Predial Urbano
  -Contribución Especial de Mejoras.
  -Planificación.
  -Rentas.
  -Recaudación.
  -Otros Impuestos (Mercados, Espacios Públicos, Cementerios, Otros).
  -Desarrollo de Aplicación Móvil para el levantamiento de Información en Campo para el Catastro Urbano.
  -Creación de Mapas temáticos en ArcGis

- Empresa / Institución: Geoinformatica Consultores
  Contratante: Dirección Nacional de Agua Potable y Saneamiento Haití
  Proyecto: "SOPORTE ESPECIALIZADO, A LA DIRECCIÓN NACIONAL DE AGUA POTABLE Y SANEAMIENTO DE HAITÍ, PARA LA REALIZACIÓN, PILOTO, DE UNA ENCUESTA POBLACIONAL CON LEVANTAMIENTO GIS EN CAMPO DE PUNTOS DE AGUA Y COBERTURA DE SANEAMIENTO"
  Papel desempeñado: Desarrollador de Aplicación Móvil para el levantamiento de Información
  Tiempo de participación: agosto 2015-diciembre 2015
  Actividades relevantes: -Desarrollo de aplicación móvil con tecnologías Híbridas en HTML5-Javascript-CSS3 con una base de datos local WebSQL,para el levantamiento de información de manera Offline, la cual se sincronice automáticamente con un servidor en la nube cuando se disponga de acceso a Internet.

- Empresa / Institución: Geoinformatica Consultores
  Contratante: ERSSAN, Paraguay
  Proyecto: Sistema Único de Información
  Papel desempeñado: Desarrollador de Módulo OpenERP
  Tiempo de participación: junio de 2015-Octubre 2015
  Actividades relevantes: -Desarrollo de Modulo de Regulación Técnica
  -Módulo Supervisión y Control
  -Módulo Económico

572

3.1.6 Documentos Técnicos

3.1.6.1 Resumen ejecutivo

TÉCNICO EN CAMPO CON EXPERIENCIA EN LA PRODUCCIÓN DE DOCUMENTOS DE IDENTIDAD NACIONALES MEDIANTE MODELO DESCENTRALIZADO DE IMPRESIÓN,

CARLOS ANDRÉS GÓMEZ GUAICHA

TÉCNICO EN CAMPO CON EXPERIENCIA EN LA PRODUCCIÓN DE DOCUMENTOS DE IDENTIDAD NACIONALES MEDIANTE MODELO DESCENTRALIZADO DE IMPRESIÓN,	**ROL**	**DETALLE DE LA EXPERIENCIA**
Técnico de campo con experiencia en producción de documentaos de identidad, pasaportes electrónicos, y la provisión de equipamiento, suscripciones-licencias de software, insumos y servicios conexos para la Dirección General de Registro Civil Identificación y cedulación (DIGERCIC)	Servicios de instalación, soporte y mantenimiento a la infraestructura de impresión a nivel nacional y países en el exterior (reparar en Nueva York (los equipos de Estados Unidos y Canadá) y en Madrid (los equipos de Europa).	**Dirección General de Registro Civil, Identificación y Cedulación** Republica de Ecuador  Vigencia: Fecha 2019 a la fecha Técnico de campo para para brindar servicios de instalación, soporte y mantenimiento a la infraestructura de impresión para la producción de documentaos de identidad, pasaportes electrónicos, y la provisión de equipamiento, suscripciones-licencias de software, insumos y servicios conexos en la Republica de Ecuador y en el exterior. Descripción de la contratación: Adquisición, implementación de un sistema informático para la emisión de documentos de identidad y pasaportes electrónicos y provisión de equipos, suscripciones – licencias de software, insumos y servicios conexos

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

		para la Dirección General de Registro Civil, Identificación y cedulación (DIGERCIC). Sistema para la emisión de documentos de identidad personal (cedula) de policarbonato y pasaportes electrónicos, PKI/ National PKD/ICAO PKD, ABIS Infraestructura de centro de datos principal y secundario, equipamiento para agencias de atención a nivel nacional y en consulados de Ecuador, para un total de 183 agencias de atención nacional para DIGERCIC y 25 agencias de Ministerio de Relaciones Exteriores y Movilidad Humana (MREMH). Descripción detallada del proyecto: Suministro, instalación y configuración de un sistema Web descentralizado para el enrolamiento Personalización y emisión de documentos de identidad Personal en Policarbonato (100%) formato ID1 y pasaportes electrónicos (EPass) formato ID3 Sistema de inspección biométrico automatizado de huellas y rostro (ABIS) para 16 millones de registros. Sistema de servicios web para búsqueda 1 a 1, 1 a N de huellas y rostros integrado al ABIS. Capacidad mínima de 10 mil a 20 mil búsquedas diarias

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo

		Infraestructura de llave pública (PKI) y su integración y conexión al Directorio de claves públicas de la OACI, se incluyeron módulos de seguridad (HSM) para el resguardo de llaves. Suministro de infraestructura (HW), licencias, suscripciones de software necesarias para la implementación de un centro de datos primario en alta disponibilidad y un sitio secundario para la recuperación de desastres. Suministro de kits – equipos de captura biométrica, producción y entrega de documentos, ambos en esquema descentralizado. Se incluyo como parte del proyecto la capacitación, transferencia de conocimientos, instalación, configuración, puesta en operación, pruebas unitarias y de integración de los sistemas centrales. Migración de la base de datos biométrica de más de 13.9 millones de registro. Este contrato incluyo el enrolamiento, personalización y emisión de pasaportes electrónicos en 25 agencias nacionales en Ecuador y 3 externas (Consulado de New York, Madrid y una oficina en Quito). Este contrato también incluyo la emisión en el Ecuador de cedulas de identidad personal en policarbonato en 183 agencias de acuerdo con los lineamientos de la OACI 9303.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo

		De igual forma incluyo servicios de post implementación, los cuales abarcan soporte técnico, mantenimiento preventivo y correctivo con niveles de servicio de 24x7x365 para todos los componentes del sistema. Importante señalar que como parte de un contrato complementario se contrató una solución de identidad digital y firma electrónica para la ciudadanía. Manejar y configurar impresoras y dispositivos de hardware.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

576

INFORMACIÓN PERSONAL

DARIO XAVIER COYAGO ARCE



Cédula de Identidad: 171267817-4

Licencia de Conducir: A, B, C1

Nacionalidad: Ecuatoriano

Edad: 37 años, 21 de Julio de 1986

Lugar de Nacimiento: Quito-Pichincha

Estado civil: Soltero

Dirección Domiciliaria: Av. La Florida N51-275 y Av. La Prensa

Teléfonos: 098-2562-651

E-MAIL: darubahhp@gmail.com, daruba_mc@hotmail.com

ASPIRACIÓN SALARIAL NETA: $1500 a $1800

PERFIL

Habilidad para realizar trabajos en equipo, capacidad de análisis, visión crítica en:

Desarrollo e investigación de software bajo lenguajes PHP, JAVA, .NET, SWIFT

Desarrollo e implementación de bases de datos en varios motores: Oracle, SQL, MySQL, Etc.

Implementación y mantenimiento a servidores, impresoras

Brindar soporte técnico, implementación de seguridad informática y precedencia de la información

Facilidad para aprender y enfrentar nuevos retos

Capacidad de comunicación a nivel verbal y escrito. Facilidad para relacionarme con diferentes tipos de personal

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

577

ESTUDIOS

SUPERIOR:
"UNIVERSIDAD TÉCNICA PARTICULAR DE LOJA"
INGENIERÍA INFORMÁTICA
Septiembre-2021

"ESCUELA POLITÉCNICA DEL EJÉRCITO"
INGENIERÍA EN SISTEMAS culminado el 8vo nivel de 10 niveles

SECUNDARIA:
Colegio **"UNIDAD EDUCATIVA F.A.E. N°1"**
Bachiller TÉCNICO ELECTROMECÁNICO
Agosto-2005

PRIMARIA:
"UNIDAD EDUCATIVA F.A.E. N°1"

FORMACIONES ADICIONALES E INTERESES

Curso de mantenimiento y ensamblaje de PC'S. **SECAP. Febrero 2005**

7mo Congreso de Ciencia y Tecnología. **ESPE. Junio-2012**

Aplicación de la Ley de Protección de Datos Personales en el Ecuador, **EICA, Julio-2023 - Duración 40 HORAS**

Máster en SQL Server: Desde Cero a Nivel Profesional 2023, **UDEMY, Octubre-2023 – Duración 16 HORAS**

Curso Power BI: De Principiante a Avanzado, **UDEMY, Enero-2024 – Duración 26.5 HORAS**

IDIOMAS

Español: Natal

Inglés: Escrito: Intermedio,
Hablado: Básico

EXPERIENCIA LABORAL

GSI INTERNATIONAL INC., Área de Sistemas. **Octubre-2023 – Actual, Quito - Ecuador**
Administrador de Base de Datos/Soporte Técnico

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

- Administrador de la base de datos al cliente DIGERCIC o Registros Civil, en el cual se verificaba el correcto funcionamiento de los servicios e infraestructura de aplicaciones, base de datos (PostgreSQL Enterprise), generación de reportes, mantenimiento a las bases de datos periódicamente.
- instalación de impresora de cedulación y de soporte a nivel nacional
- Desarrollo de software Back-end y Front-end uso interno, PHP, JavaScript, Boostrap, los cuales se realizaron para emisión de reportes, consultas de estados, y generación de informes.

TESQUIMSA C.A., Área de Sistemas. **Julio-2021 – Octubre-2023, Quito - Ecuador**

Jefe de Sistemas

- Elaborar planes, programas y proyectos informáticos de la entidad.
- Elaborar el portafolio de desarrollo de soluciones tecnológicas propias, adquiridas y/o adaptadas y proyectos informáticos gestionados.
- Elaborar informes de validación de términos de referencia, especificaciones funcionales y técnicas para la contratación proyectos de T.I.
- Elaborar informes de gestión de paso a producción de los proyectos informáticos desarrollados o implantados.
- Elaborar Bitácoras de incidentes atendidos y no atendidos de segundo y tercer nivel.
- Elaborar Informes de administración, transferencia de conocimiento y fiscalización de sistemas informáticos, servicios web, consultorías y contratos requeridos por la empresa.

INSTITUTO SUPERIOR TECNOLOGICO CRUZ ROJA ECUATORIANA, Área de Sistemas. **Octubre-2018 – Octubre-2020, Quito - Ecuador**

Encargado de Desarrollo

- Soporte Técnico, mantenimiento y desarrollo de software, utilización de
- herramientas de programación y de comunicación como; lectores de barras,
- biométricos. Desarrollo en el lenguaje de PHP, .NET, Java.
- Administrador de bases de datos: Oracle, MySQL, instalación de impresora de cedulación y de soporte a nivel nacional
- Implementación y mantenimiento de servidores de aplicaciones y de bases de datos.

ALGORITMUN S.A., Área de Sistemas. **Enero-2018 – Julio-2018, Quito – Ecuador**

Encargado de Desarrollo

- Mantenimiento y desarrollo de software, utilización de herramientas de programación y de comunicación como, lector de barras. Desarrollo en el lenguaje de PHP, PYTHON.

AZULEC S.A., Área de Sistemas. **Enero-2014 – Noviembre-2017, Quito - Ecuador**

Encargado de Desarrollo

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

Tareas realizadas: Mantenimiento y desarrollo de software, utilización de herramientas de programación y de comunicación como biométrico, lector de barras. Desarrollo en el lenguaje de PHP, JAVA, C#, entre otros. Desarrolle del sistema de facturación electrónica ON-LINE y OFF-LINE.

BIP CONSULTORES, Área de Sistemas. **Julio-2015 – Julio-2016 Quito - Ecuador**
Asistente de TI
Tareas realizadas: Desarrollo sistema de medición y mejora para un Sistema de Gestión de Calidad bajo la Norma ISO 9001.
Desarrollo sistema de gestión Documental
Desarrollo sistema de Recursos Humanos
Desarrollo sistema de Nómina

ECUAQUIMICA, Área de Sistemas **Junio-2013 – Noviembre-2013 Quito - Ecuador**
Asistente de TI
Tareas realizadas: Desarrollo en JAVA JSF para el sistema de uso en la Organización.

HOTEL MELLROSE-PLAZA, Área de Sistemas **Mayo-2015 – Mayo-2015 Quito - Ecuador**
Asistente de TI
Tareas realizadas: Reconfiguración de la red interna.

Ing. José Pérez (Halliburton), Área de Sistemas **Abril-2014 – Abril-2015 Quito - Ecuador**
Asistente de TI
Tareas realizadas: Recuperación de información perdida, e instalación de cámara de seguridad

COMREIVIC, Área de Sistemas **Abril-2011 – Julio 2012 Quito - Ecuador**
Pasante
Tareas realizadas: Soporte técnico, mantenimiento de Hardware y software, administración de redes, ayuda personalizada y remota a los usuarios.

CONOCIMIENTOS

Microsoft Office & OpenOffice
Manejo de las herramientas y soporte a usuario
Manejo Avanzado.

Base de Datos
Manejo de cubos de información, Administración, Mineria de datos, Oracle, SQL-SERVER, MYSQL, PostgreSQL **Manejo Avanzado**

Herramientas Graficas

CONSORCIO EMDOC
EMDOC CONSORCIO
Santo Domingo, R.D.

Tratamiento de multimedia mediante ADOBE CS6 **Manejo Básico**

Web Services REST
Implementación y configuración de aplicaciones **Manejo Intermedio**

Manejo de REDES
Gestión de redes, estructurarlas y administrarlas **Manejo Intermedio**

Mantenimiento correctivo y preventivo Pc
Actividades de reparación y optimización de la PC tanto en el hardware y software, reparación de ciertos dispositivos con resultados excelentes **Manejo Avanzado.**

Programación JAVA
Programación orientada a objetos y desarrollo de software JSF **Manejo Intermedio.**

Programación .NET
Desarrollo de proyectos en visual, C# **Manejo Avanzado.**

Programación PHP, JAVASCRIPT, JQUERY, AJAX
Implementación de proyectos, en lo referente al desarrollo de páginas web diseñadas en código PHP utilizando framework CodeIgniter, de acuerdo con las necesidades del cliente **Manejo Avanzado.**

HTML5, CSS3, Bootstrap 3
Implementación de proyectos, en lo referente al desarrollo de páginas web diseñadas en la parte del frontend **Manejo Avanzado.**

HERRAMIENTAS DE APRENDIZAJE
Desarrollo, configuración y manejo en herramientas de aprendizaje como: Canvas, Moodle, Edmodo, Microsoft Teams. **Manejo Intermedio.**

Programación XCODE
Desarrollo de aplicaciones utilizando las herramientas de Xcode, en el lenguaje de programación SWIFT para MAC. **Manejo Básico.**

Programación Access, Macros
Desarrollo de proyectos, con macros y uso de base de datos Access. **Manejo Intermedio.**

Informática Forense
Identificación, preservación y análisis de la información para un proceso legal.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

Recuperación de información perdida en dispositivos de almacenamiento.
Manejo de diferentes sistemas para seguridades en el sistema y la red **Manejo Intermedio.**

Implementación de servidores

Implementación y levantamiento de varios servicios, tanto de aplicaciones, como de bases de datos, mantenimiento físico y lógico de los servidores. **Manejo Intermedio.**

Implementación de la Ley de Protección de Datos Personales

Implementación y levantamiento de procesos referente a la ley de protección de datos personales, desarrollo en la página y sus diferentes clausulas y protecciones, generación de matrices. **Manejo Intermedio.**

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

582

3.1.6 Documentos Técnicos

3.1.6.1 Resumen ejecutivo

TÉCNICO EN CAMPO CON EXPERIENCIA EN LA PRODUCCIÓN DE DOCUMENTOS DE IDENTIDAD NACIONALES MEDIANTE MODELO DESCENTRALIZADO DE IMPRESIÓN,

Dario Xavier Coyago Arce

TÉCNICO EN CAMPO CON EXPERIENCIA EN LA PRODUCCIÓN DE DOCUMENTOS DE IDENTIDAD NACIONALES MEDIANTE MODELO DESCENTRALIZADO DE IMPRESIÓN,	**ROL**	**DETALLE DE LA EXPERIENCIA**
Técnico de campo con experiencia en producción de documentaos de identidad, pasaportes electrónicos, y la provisión de equipamiento, suscripciones-licencias de software, insumos y servicios conexos para la Dirección General de Registro Civil Identificación y cedulación (DIGERCIC)	Servicios de instalación, soporte y mantenimiento a la infraestructura de impresión a nivel nacional y países en el exterior (reparar en Nueva York (los equipos de Estados Unidos y Canadá) y en Madrid (los equipos de Europa).	**Dirección General de Registro Civil, Identificación y Cedulación** Republica de Ecuador  Vigencia: Fecha 2019 a la fecha Técnico de campo para para brindar servicios de instalación, soporte y mantenimiento a la infraestructura de impresión para la producción de documentaos de identidad, pasaportes electrónicos, y la provisión de equipamiento, suscripciones-licencias de software, insumos y servicios conexos en la Republica de Ecuador y en el exterior. Descripción de la contratación: Adquisición, implementación de un sistema informático para la emisión de documentos de identidad y pasaportes electrónicos y provisión de equipos, suscripciones – licencias de software, insumos y servicios conexos para la Dirección General de Registro Civil, Identificación y cedulación (DIGERCIC).

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

		Sistema para la emisión de documentos de identidad personal (cedula) de policarbonato y pasaportes electrónicos, PKI/ National PKD/ICAO PKD, ABIS Infraestructura de centro de datos principal y secundario, equipamiento para agencias de atención a nivel nacional y en consulados de Ecuador, para un total de 183 agencias de atención nacional para DIGERCIC y 25 agencias de Ministerio de Relaciones Exteriores y Movilidad Humana (MREMH). Descripción detallada del proyecto: Suministro, instalación y configuración de un sistema Web descentralizado para el enrolamiento Personalización y emisión de documentos de identidad Personal en Policarbonato (100%) formato ID1 y pasaportes electrónicos (EPass) formato ID3 Sistema de inspección biométrico automatizado de huellas y rostro (ABIS) para 16 millones de registros. Sistema de servicios web para búsqueda 1 a 1 y 1 a N de huellas y rostros integrado al ABIS. Capacidad mínima de 10 mil a 20 mil búsquedas diarias Infraestructura de llave pública (PKI) y su integración y conexión al Directorio de claves públicas de la OACI, se incluyeron módulos de seguridad (HSM) para el resguardo de llaves. Suministro de infraestructura (HW), licencias, suscripciones de software necesarias para la

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

		implementación de un centro de datos primario en alta disponibilidad y un sitio secundario para la recuperación de desastres. Suministro de kits – equipos de captura biométrica, producción y entrega de documentos, ambos en esquema descentralizado. Se incluyo como parte del proyecto la capacitación, transferencia de conocimientos, instalación, configuración, puesta en operación, pruebas unitarias y de integración de los sistemas centrales. Migración de la base de datos biométrica de más de 13.9 millones de registro. Este contrato incluyo el enrolamiento, personalización y emisión de pasaportes electrónicos en 25 agencias nacionales en Ecuador y 3 externas (Consulado de New York, Madrid y una oficina en Quito). Este contrato también incluyo la emisión en el Ecuador de cedulas de identidad personal en policarbonato en 183 agencias de acuerdo con los lineamientos de la OACI 9303. De igual forma incluyo servicios de post implementación, los cuales abarcan soporte técnico, mantenimiento preventivo y correctivo con niveles de servicio de 24x7x365 para todos los componentes del sistema. Importante señalar que como parte de un contrato complementario se contrató una solución de identidad digital y firma electrónica para la ciudadanía.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

		Manejar y configurar impresoras y dispositivos de hardware.

CONSORCIO EMDOC
Santo Domingo

Certificaciones ISO

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

ISO 14928 INTERGRAF o equivalente nivel gobierno

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

JOSÉ MIGUEL GUERRA GONZÁLEZ
Intérprete Judicial

Yo, José Miguel Guerra González, Intérprete Judicial del Juzgado de Primera Instancia del Distrito Nacional, República Dominicana, debidamente juramentado para el ejercicio de mis funciones, CERTIFICO: Que he traducido un documento escrito en inglés cuya versión en español, a mi mejor entender, es la siguiente:

Copia Certificada

Certificado INTERGRAF para la Gestión de la Seguridad de los Procesos de Impresión

Intergraf por este medio certifica que, basado en los resultados de la auditoría realizada por VPGI Certification B.V., La Haya, Países Bajos,

Mühlbauer ID Services GmbH
Josef Mühlbauer Platz 1, 93426 Roding, Alemania

cumple con la norma ISO 14298:2021 "Gestión de Seguridad de los Procesos de Impresión" y con los requerimientos correspondientes de Intergraf para esta norma.

Nivel de certificación:	Nivel Gubernamental
Mercados de operación:	Nacional, Internacional Organizaciones No Gubernamentales y Gubernamentales
Marco:	Producción de documentos de identificación tales como Pasaportes/Pasaportes Electrónicos, tarjetas de identificación y documentos relacionados, incluyendo la pre personalización.

Número de referencia del certificado: 202303649
Fecha de expiración: 25 de mayo de 2026

Bruselas, 31 de mayo de 2023

[Sello: Certificado - *Ilegible*]

Por Intergraf

[Firmado]
Beatrice Klose
Secretaria General

[Sello: Intergraf]

Por VPGI

[Firmado]
Marc Been
Director General

[Sello: VPGI]

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

589

Por este medio certifico que la anterior es una copia fiel del original que ha sido presentado por ante mi.

Roding, 19 de junio de 2023

[Firmado]
Benjamin Weingarten
Notario Público
(licencia vitalicia)

[Sello: Benjamin Weingarten, Notario de Roding]

No. de archivo 91 E 203/2024

Por este medio certifico la autenticidad de la firma que precede del **Notario Benjamin Weingarten de Roding,**

así como la autenticidad del sello oficial añadido.

Además, certifico que la persona antes mencionada está legalmente autorizada a ejecutar este acto oficial.

Ratisbona, el 12 de junio de 2024
La Presidenta del Tribunal Regional
De orden

[Firmado]
Ingrid Schwarz
Inspectora de la Administración de Justicia

[Sello: Tribunal Regional de Ratisbona, Baviera]

Desglose de Costos
Impuesto: 25.00 €
(según el Art. 1, Párrafo 1 de la Ley de Costos Judiciales Estatales (LJKostG), en conjunto con la Sección 4, Párrafo 1 de la Ley de Costos de la Administración Judicial (JVKostG), KV 13.10)

El documento que antecede fue traducido en Santo Domingo, capital de la República Dominicana, el día 26 de julio del año 2024, y está registrado en mis archivos como "Certificado de Norma ISO 14298:2021 MÜHLBAUER ID SERVICES GMBH 2024072601".

JOSÉ MIGUEL GUERRA GONZÁLEZ
Intérprete Judicial
Tralega Traducciones Legales, Intérpretes Judiciales
809-535-3011 / 809-535-6011 © tralega.com info@tralega.com

Certified Copy

590

INTERGRAF Certificate for Management of Security Printing Processes

Intergraf hereby certifies that, based on the results of the audit conducted by VPGI Certification B.V., The Hague, The Netherlands,

Mühlbauer ID Services GmbH

Josef Mühlbauer Platz 1, 93426 Roding, Germany

complies with ISO 14298:2021 "Management of Security Printing Processes" and with the relevant Intergraf requirements for this standard.

Certification Level:	Governmental level
Markets of Operation:	National, International Non-Governmental and Governmental organizations
Scope:	Production of identification documents such as Passports/ePassports, ID cards and related documents including the pre-personalization.

Reference Number of the Certificate: 202303649
Expiration Date: 25 May 2026

Brussels, 31 May 2023

For Intergraf

INTERGRAF

Beatrice Klose
Secretary General

For VPGI

Marc Been
Managing Director

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

591

I hereby certify that the above is a true copy of the original which has been presented to me.
Roding, 19. JUNI 2023
Benjamin Weingarten
Notary Public
[the seal / stamp]

Gz. 91 E 203/2024

Die Echtheit vorstehender Unterschrift von

Notar Benjamin Weingarten
in Roding

und die Echtheit des beigedrückten Dienstsiegels
werden hiermit bestätigt.

Zugleich wird bescheinigt, dass der/die Vorgenannte
zur Vornahme der Amtshandlung gesetzlich befugt war.

Regensburg, den 12. Juni 2024
Der Präsident des Landgerichts
Im Auftrag
Ingrid Schwarz
Justizverwaltungsinspektorin

Kostenrechnung
Gebühr: 25,00 €
(gem. Art. 1 Abs. 1 LJKostG, i.V.m.
§ 4 Abs. 1 JVKostG, KV 13.10

592

Stiftstr.2, 60313 Frankfurt am Main, Alemania,
Tel.:49 69 74 38 77 81 | Fax: 49 69 74 38 78 42
www.consuladodominicanofrkf@hotmail.com

Consulado General
de la República Dominicana
en Frankfurt, Alemania

Reg.00263/2024

CONSULADO GENERAL DE LA REPUBLICA DOMINICANA EN FRANKFURT, ALEMANIA.

CERTIFICO Y DOY FE (sin entrar en el contenido del documento ni ulterior destino que pueda dársele): que la firma que aparece al pie de **ESTE CERTIFICADO**, Identificado con el **No. S/N**, de fecha **10 DE JUNIO DEL 2024,** corresponde **A LA SRA. INGRID SCHWARZ, PRESIDENTE DE LA AUDIENCIA PROVINCIAL**, de la ciudad de REGENSBURG, Alemania.

Y que es la Firma que acostumbra a usar en todos sus actos y a la cual se debe entera fe y crédito.

En Frankfurt am Main, Alemania, a los dieciocho (18) dias del mes de junio del año dos mil veinticuatro (2024).

Niovel Aurora Tapia Ortiz
Vicecónsul

CONSULADO GENERAL DE LA REPUBLICA DOMINICANA
FRANKFURT, ALEMANIA

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

CONSORCIO EMDOC
EMDOC CONSORCIO
Santo Domingo, RD

594

República Dominicana

MINISTERIO DE RELACIONES EXTERIORES

Viceministerio para Asuntos Consulares y Migratorios

Dirección de Legalización de Documentos

APOSTILLA

(Convention de la Haye du 5 octobre 1961)

1.País:
Country / Pays: REPÚBLICA DOMINICANA

El presente documento público
This public document / Le présent acte public

2.Ha sido firmado por:
Has been signed by / A été signé par: NIOVEL AURORA TAPIA ORTIZ

3.Quien actúa en calidad de:
Acting in the capacity of / Agissant en qualité de: VICECÓNSUL

4.Y está revestido del sello / timbre de:
Bears the seal / stamp of
Est revêtu du sceau / timbre de: CONSULADO GENERAL DE LA REPUBLICA DOMINICANA EN FRANKFURT, REPUBLICA FEDERAL DE ALEMANIA

Certificado
Certified / Attesté

5.En:
At / À: SANTO DOMINGO

6.El día:
The / Le: 28/7/2024

7.Por:
By / Par: OPINIO ANTONIO DIAZ VARGAS - VICEMINISTRO ASUNTOS CONSULARES Y MIGRATORIOS

8.Bajo el número:
N° / Sous: AP-2024-7-28-41

9.Sello / Timbre:
Seal / Stamp
Sceau / Timbre

10.Firma:
Signature

Verificación Verification / Vérification			
País Destino:	REPÚBLICA DOMINICANA	**Código de verificación:**	DF8GD6EXJF76HL2

Esta Apostilla certifica únicamente la autenticidad de la firma, la calidad en que el signatario del documento haya actuado, y en su caso, la identidad del sello o timbre del que el documento público este revestido.

This Apostille only certifies the authenticity of the signature and the capacity of the person who has signed the public document, and, where appropriate, the identity of the seal or stamp which the public document bears.

Cette Apostille atteste uniquement la véracité de la signature, la qualité en laquelle le signataire de l'acte a agi et, le cas échéant, l'identité du sceau ou timbre dont cet acte public est revêtu.

CONSORCIO EMDOC Santo Domingo, R.D.

595

ISO 27001:2013

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

596

JOSÉ MIGUEL GUERRA GONZÁLEZ
Intérprete Judicial

Yo, José Miguel Guerra González, Intérprete Judicial del Juzgado de Primera Instancia del Distrito Nacional, República Dominicana, debidamente juramentado para el ejercicio de mis funciones, CERTIFICO: Que he traducido un documento escrito en inglés y alemán cuya versión en español, a mi mejor entender, es la siguiente:

Copia Certificada

DEKRA

CERTIFICADO

MÜHLBAUER High Tech International

DIN EN ISO/IEC 27001:2017
Equivalente técnico a la ISO/IEC 27001:2013 incluyendo Cor 1:2014 y Cor 2:2015

DEKRA Certification GmbH por la presente certifica que la organización

Mühlbauer ID Services GmbH

Josef-Mühlbauer-Platz 1, 93426 Roding, Alemania

para la cobertura de la certificación:

Desarrollo de hardware y software en el ámbito de soluciones de gobierno electrónico. Prestación de servicios de consultoría, soporte y formación en el ámbito de soluciones de gobierno electrónico. Prestación de servicios de centros de datos para el desarrollo de hardware y software.

(ver ubicaciones en el anexo)

ha establecido y mantiene un sistema de gestión de seguridad de la información de acuerdo con el estándar mencionado anteriormente y a la declaración de aplicabilidad de fecha 31/01/24, revisión V240131. El cumplimiento se registró con el informe de auditoria No. A23101492.

No. de registro del certificado:	DS-0512011/4
Vigencia del certificado anterior:	24/05/2024
Certificado válido desde:	12/06/2024
Certificado válido hasta:	31/10/2025

[Firmado] [Sello: DEKRA Certification GmbH - D-70565 Stuttgart Handwerkstraße 15]
Dr. Rolf Krökel
DEKRA Certification GmbH, Stuttgart, 12/06/2024

Miembro del Acuerdo Multilateral de Reconocimiento IAF

DAKKS Organismo de Acreditación de [illegible]

CONSORCIO EMDOC
EMDOC CONSORCIO
Santo Domingo, R.D.

DEKRA

Anexo al certificado No. DS-0512011/4

válido del 12/06/2024 al 31/10/2025

Las siguientes ubicaciones/organizaciones pertenecen al certificado anterior:

	Sede		**Cobertura de la certificación**
	Mühlbauer ID Services GmbH	Josef-Mühlbauer-Platz 1 93426 Roding Alemania	Ver página 1
	en las siguientes ubicaciones / en las organizaciones en las siguientes ubicaciones		**Cobertura de la certificación**
1.		Manfred-von-Ardenne-Ring 15 01099 Dresde Alemania	Desarrollo de software para la captura y procesamiento de datos biométricos para documentos de identidad en el ámbito de soluciones de gobierno electrónico. Prestación de servicios de consultoría, soporte y formación en el ámbito de soluciones de gobierno electrónico.
2.		Bahnhofstraße 1-3 58095 Hagen Alemania	Desarrollo de software para la captura y procesamiento de datos biométricos para documentos de identidad en el ámbito de soluciones de gobierno electrónico. Prestación de servicios de consultoría, soporte y formación en el ámbito de soluciones de gobierno electrónico.
3.		Industriestraße 15 18069 Rostock Alemania	Desarrollo de software para la captura y procesamiento de datos biométricos para documentos de identidad en el ámbito de soluciones de gobierno electrónico. Prestación de servicios de consultoría, soporte y formación en el ámbito de soluciones de gobierno electrónico.

[Firmado] [Sello: DEKRA Certification GmbH - D-70565 Stuttgart Handwerkstraße 15]
Dr. Rolf Krökel
DEKRA Certification GmbH, Stuttgart, 12/06/2024

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

57

La copia anterior corresponde al documento original.

Roding, 19 de junio de 2024

[Firmado]
Notaria
[Sello: Katharina Marchner, Notaria de Roding]

No. de archivo 91 E 207/2024

Por este medio certifico la autenticidad de la firma que precede de la **Notaria Katharina Marchner de Roding,**

así como la autenticidad del sello oficial añadido.

Además, certifico que la persona antes mencionada está legalmente autorizada a ejecutar este acto oficial.

Ratisbona, el 19 de junio de 2024
La Presidenta del Tribunal Regional
De orden

[Firmado]
Manuela Wanner
Oficial Judicial

[Sello: Tribunal Regional de Ratisbona, Baviera]

Desglose de Costos
Impuesto: 25.00 €
(según el Art. 1, Párrafo 1 de la Ley de Costos Judiciales Estatales (LJKostG), en conjunto con la Sección 4, Párrafo 1 de la Ley de Costos de la Administración Judicial (JVKostG), KV 13.10)

El documento que antecede fue traducido en Santo Domingo, capital de la República Dominicana, el día 26 de julio del año 2024, y está registrado en mis archivos como "Certificado de Norma ISO/IEC 27001:2017 MÜHLBAUER ID SERVICES GMBH 2024072602".

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, D.N.

Lic. José Miguel Guerra González
INTÉRPRETE JUDICIAL DEL JUZGADO DE PRIMERA INSTANCIA
República Dominicana

JOSÉ MIGUEL GUERRA GONZÁLEZ
Intérprete Judicial
Tralega Traducciones Legales, Intérpretes Judiciales
809-535-3011 / 809-535-6011 tralega.com info@tralega.com

Beglaubigte Ablichtung

599

CERTIFICATE

Mühlbauer
High Tech International

DIN EN ISO/IEC 27001:2017

Technical equivalent to ISO/IEC 27001:2013 including Cor 1:2014 and Cor 2:2015

DEKRA Certification GmbH hereby certifies that the organization

Mühlbauer ID Services GmbH

Josef-Mühlbauer-Platz 1, 93426 Roding, Germany

for the scope of certification:

Development of hardware and software in the field of e-government solutions.
Provision of consulting, support and training services in the field of e-government solutions.
Provision of data center services for hardware and software development.

(sites see annex)

has established and maintains an information security management system according to the above mentioned standard and to the statement of applicability from 31.01.24, revision V240131. The conformity was adduced with audit report no. A23101492.

Certificate registration no.:	DS-0612011/4
Validity of previous certificate:	2024-06-24
Certificate valid from:	2024-06-12
Certificate valid to:	2025-10-31

DEKRA

Dr. Rolf Krokel
DEKRA Certification GmbH, Stuttgart, 2024-06-12

CONSORCIO EMDOC
EMDOC
Santo Domingo, R.D.

600

Annex to the certificate no. DS-0512011/4

valid from 2024-06-12 to 2025-10-31

The following sites / organizations belong to the certificate above:

	Headquarters		Scope of certification
	Mühlbauer ID Services GmbH	Josef-Mühlbauer-Platz 1 93426 Roding Germany	See page 1
	at the following sites / at the organizations at the following sites		**Scope of certification**
1.		Manfred-von-Ardenne-Ring 15 01099 Dresden Germany	Development of software for capturing and processing biometric data for ID documents in the field of e-government solutions. Provision of consulting, support and training services in the field of e-government solutions
2.		Bahnhofstraße 1-3 58095 Hagen Germany	Development of software for capturing and processing biometric data for ID documents in the field of e-government solutions. Provision of consulting, support and training services in the field of e-government solutions
3.		Industriestraße 15 18069 Rostock Germany	Development of software for capturing and processing biometric data for ID documents in the field of e-government solutions. Provision of consulting, support and training services in the field of e-government solutions

DEKRA

Dr. Rolf Krckel
DEKRA Certification GmbH, Stuttgart, 2024-06-12

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo - R.D.

601

Die Abschrift stimmt mit der Urschrift überein.
Roding, 19. JUNI 2024
Notarin

Gz. 91 E 207/2024

Die Echtheit vorstehender Unterschrift von

Notarin Katharina Marchner in Roding

und die Echtheit des beigedrückten Dienstsiegels werden hiermit bestätigt.

Zugleich wird bescheinigt, dass der/die Vorgenannte zur Vornahme der Amtshandlung gesetzlich befugt war.

Regensburg, den 19. Juni 2024
Der Präsident des Landgerichts
Im Auftrag

Manuela Wanner
Justizangestellte

BAYERN · AMTSGERICHT REGENSBURG

Kostenrechnung
Gebühr: 25,00 €
(gem. Art. 1 Abs. 1 LJKostG, i.V.m. § 4 Abs. 1 JVKostG, KV 11.10)

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

602

Consulado General
de la República Dominicana
en Frankfurt, Alemania

Stiftstr.2, 60313 Frankfurt am
Tel.:49 69 74 30 77 81 / Fax: 49 6
www.consuladodominicanoderm@

Reg.00286/2024

CONSULADO GENERAL DE LA REPUBLICA DOMINICANA EN FRANKFURT, ALEMANIA.

CERTIFICO Y DOY FE (sin entrar en el contenido del documento ni ulterior destino que pueda dársele): que la firma que aparece al pie de **ESTA COPIA NOTARIAL**, Identificado con el **No. S/N**, de fecha **19 DE JUNIO DEL 2024,** corresponde **A LA SRA. MANUELA WANNER, PRESIDENTE DE LA AUDIENCIA PROVINCIAL**, de la ciudad de REGENSBURG, Alemania.

Y que es la Firma que acostumbra a usar en todos sus actos y a la cual se debe entera fe y crédito.

En Frankfurt am Main, Alemania, a los veintiún (21) dias del mes de junio del año dos mil veinticuatro (2024).

Niovel Aurora Tapia Ortiz
Vicecónsul

CONSULADO GENERAL DE LA REPUBLICA DOMINICANA FRANKFURT, ALEMANIA

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

60

603

CONSORCIO EMDOC

EMDOC

Santo Do... R.D.

604

República Dominicana
MINISTERIO DE RELACIONES EXTERIORES
Viceministerio para Asuntos Consulares y Migratorios
Dirección de Legalización de Documentos

APOSTILLA

(Convention de la Haye du 5 octobre 1961)

1.País:
Country / Pays: REPÚBLICA DOMINICANA

El presente documento público
This public document / Le présent acte public

2.Ha sido firmado por:
Has been signed by / A été signé par: NIOVEL AURORA TAPIA ORTIZ

3.Quien actúa en calidad de:
Acting in the capacity of / Agissant en qualité de: VICECÓNSUL

4.Y está revestido del sello / timbre de:
Bears the seal / stamp of
Est revêtu du sceau / timbre de: CONSULADO GENERAL DE LA REPUBLICA DOMINICANA EN FRANKFURT, REPUBLICA FEDERAL DE ALEMANIA

Certificado
Certified / Attesté

5.En:
At / À: SANTO DOMINGO

6.El día:
The / Le: 28/7/2024

7.Por:
By / Par: OPINIO ANTONIO DIAZ VARGAS - VICEMINISTRO ASUNTOS CONSULARES Y MIGRATORIOS

8.Bajo el número:
N° / Sous: AP-2024-7-28-27

9.Sello / Timbre:
Seal / Stamp
Sceau / Timbre

10.Firma:
Signature

Verificación
Verification / Vérification

País Destino:	REPÚBLICA DOMINICANA	**Código de verificación:**	K2GHTRDC2XA5KJY

Esta Apostilla certifica únicamente la autenticidad de la firma, la calidad en que el signatario del documento haya actuado, y en su caso, la identidad del sello o timbre del que el documento público este revestido.

This Apostille only certifies the authenticity of the signature and the capacity of the person who has signed the public document, and, where appropriate, the identity of the seal or stamp which the public document bears.

Cette Apostille atteste uniquement la véracité de la signature, la qualité en laquelle le signataire de l'acte a agi et, le cas échéant, l'identité du sceau ou timbre dont cet acte public est revêtu.

9

605

ISO 14001 o equivalente

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

Beglaubigte Ablichtung

606

CERTIFICATE

Mühlbauer
High Tech International

ISO 14001:2015

DEKRA Certification GmbH hereby certifies that the organization

Mühlbauer ID Services GmbH

Josef-Mühlbauer-Platz 1, 93426 Roding, Germany

for the scope of certification:

Development of hardware and software in field of e-government solutions,
provision of consulting, support and training services
in the field of e-government solutions,
provision of data center service for hardware and software development

has established and maintains an environmental management system according to the above mentioned standard. The conformity was adduced with audit report no. A23101081

Certificate registration no.:	170923134/1
Validity of previous certificate:	2024-08-26
Certificate valid from:	2024-08-27
Certificate valid to:	2027-08-15

DEKRA

Dr. Rolf Krokel
DEKRA Certification GmbH, Stuttgart, 2024-08-27

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

607

Die Ablichtung stimmt mit der Urschrift überein.
Roding, 03. FEB. 2025
Notarin

Ref.No. 91 E 37/2025

I hereby certify the authenticity of the above signature of the notary public

Notarin Katharina Marchner
in Roding

and the authenticity of the stamped official seal.

Furthermore, I certify that the person cited above was legally authorized of perform official duty.

Regensburg, the 07th day of February, 2025
The President of the Regional Court
by proxy
Ingrid Schwarz
Judical Administration Inspector

Cost account
Fixed charge: 25,00 €
(according to Art. 1(1) State Justice Costs Act (LJKostG) in conjunction with § 4
Judical Administration Costs Act (JVKostG), statement of charges 13

608

República Dominicana
MINISTERIO DE RELACIONES EXTERIORES
Viceministerio para Asuntos Consulares y Migratorios
Dirección de Legalización de Documentos

APOSTILLA

(Convention de la Haye du 5 octobre 1961)

1.País:
Country / Pays: REPÚBLICA DOMINICANA

El presente documento público
This public document / Le présent acte public

2.Ha sido firmado por:
Has been signed by / A été signé par: NIOVEL AURORA TAPIA ORTIZ

3.Quien actúa en calidad de:
Acting in the capacity of / Agissant en qualité de: VICECÓNSUL

4.Y está revestido del sello / timbre de:
Bears the seal / stamp of
Est revêtu du sceau / timbre de: CONSULADO GENERAL DE LA REPUBLICA DOMINICANA EN FRANKFURT, REPUBLICA FEDERAL DE ALEMANIA

Certificado
Certified / Attesté

5.En: At / À	SANTO DOMINGO	**6.El día:** The / Le	26/7/2024
7.Por: By / Par	OPINIO ANTONIO DIAZ VARGAS - VICEMINISTRO ASUNTOS CONSULARES Y MIGRATORIOS	**8.Bajo el número:** N° / Sous°	AP-2024-7-28-14
9.Sello / Timbre: Seal / Stamp Sceau / Timbre		**10.Firma:** Signature	

Verificación
Verification / Vérification

País Destino:	REPÚBLICA DOMINICANA	Código de verificación:	CVUE9E2FNZRJ87P

Esta Apostilla certifica únicamente la autenticidad de la firma, la calidad en que el signatario del documento haya actuado, y en su caso, la identidad del sello o timbre del que el documento público está revestido.

This Apostille only certifies the authenticity of the signature and the capacity of the person who has signed the public document, and, where appropriate, the identity of the seal or stamp which the public document bears.

Cette Apostille atteste uniquement la véracité de la signature, la qualité en laquelle le signataire de l'acte a agi et, le cas échéant, l'identité du sceau ou timbre dont cet acte public est revêtu.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

Consulado General
de la República Dominicana
en Frankfurt, Alemania

Stiftstr.2, 60313 Frankfurt am Main, Alemania.
Tel.:49 69 74 30 77 81 / Fax: 49 69 74 30 76 40
www.consuladodominicanoffm@hotmail.com

609

AP-2024-7-28-14

Reg.00265/2024

CONSULADO GENERAL DE LA REPUBLICA DOMINICANA EN FRANKFURT, ALEMANIA.

CERTIFICO Y DOY FE (sin entrar en el contenido del documento ni ulterior destino que pueda dársele): que la firma que aparece al pie de **ESTE CERTIFICADO**, Identificado con el **No. S/N**, de fecha **19 DE SEPTIEMBRE DEL 2023,** corresponde **A LA SRA. INGRID SCHWARZ, PRESIDENTE DE LA AUDIENCIA PROVINCIAL**, de la ciudad de REGENSBURG, Alemania.

Y que es la Firma que acostumbra a usar en todos sus actos y a la cual se debe entera fe y crédito.

En Frankfurt am Main, Alemania, a los dieciocho (18) dias del mes de junio del año dos mil veinticuatro (2024).

Nibvel Aurora Tapia Ortiz
Vicecónsul

CONSULADO GENERAL DE LA REPUBLICA DOMINICANA
FRANKFURT, ALEMANIA

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

610

054-2025

Yo, **Virginia Wall Guerra**, Intérprete Judicial de la República Dominicana, debidamente juramentada por el Consejo del Poder Judicial, titular de la cédula de identidad y electoral número 001-1637246-7, matricula 47144, certifico que he traducido un documento cuyo original se encuentra en los idiomas INGLÉS y ALEMÁN, marcado en mi protocolo con número 054-2025, cuyo texto en el idioma ESPAÑOL se leería de la forma siguiente:

[página 1]

Copia certificada

CERTIFICADO

[logo] Mühlbauer
High Tech International

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo R.D.

ISO 14001 : 2015

Dekra Certification GmbH certifica por este medio que la organización

Mühlbauer ID Services GmbH
Josef-Mühlbauer-Platz 1, 93426, Roding, Alemania,

para el ámbito de la certificación:

Desarrollo de hardware y software en el campo de las soluciones de gobierno electrónico. Prestación de servicios de consultoría, soporte y formación en el ámbito de las soluciones de gobierno electrónico. Proporcionar servicios de centro de datos para el desarrollo de hardware y software.

ha establecido y mantiene un sistema de gerencia de calidad de acuerdo al estándar mencionado arriba. La conformidad se adujo del informe de auditoría no. A23101081

No de registro del certificado	170923134/1
Validez del certificado anterior	2024-08-26
Certificado válido desde:	2024-08-27
Certificado válido hasta	2027-08-15

Traducción de idioma
[firma ilegible]
Dr. Rolf Kröket
DEKRA Certification GmbH, Berlin
2024-08-27

[sello redondo] *[logo]* *[logo]*
DEKRA Certification GmbH

Virginia Wall Guerra Intérprete Judicial de la República Dominicana 1/3 Ruso e Inglés

[pie de página]
DEKRA Certification GmbH * Handwerkstraße 15* D-70565 Stuttgart * www.dekra-certification.de

611

[página 2]

[sello redondo ilegible]
KATHARINA MARCHNER
NOTARIO EN RODING

La copia anterior corresponde a los extractos relevantes del original.
En Roding, el 03 de febrero de 2025

[firma ilegible]
Notario

Protocolo 91 E 37/2025

Por la presente se confirma la autenticidad de la firma de la Notario **Katharina Marchner, en Roding** y la autenticidad del sello oficial adjunto.

Al mismo tiempo, se certifica que la referida persona estaba legalmente autorizada para realizar el acto oficial.

En Regensburg, el 07 de febrero de 2025
El Presidente del Tribunal Provincial
De Orden
[firma ilegible] Ingrid Schwarz
Inspectora de Administración de Justicia

[sello redondo]
BAVARIA- TRIBUNAL PROVINCIAL DE REGENSBURG

Cálculo de costos
Tasa: 25.00 euros
(de acuerdo al art. 1, párrafo 1 de la Ley de Costas Judiciales
Sección 4, párrafo 1 de la Ley de Costas Judiciales KV 13.10

[texto en español]

[escudo]
Consulado General de la República Dominicana
En Frankfurt, Alemania

Certifica: Visto bueno para legalizar la firma y sello de INGRID SCHWARZ, PRESIDENTE DE LA AUDIENCIA PROVINCIAL DE LA CIUDAD DE REGENSBURG, ALEMANIA., por ser, al parecer, auténtica sin prejuzgar la veracidad del contenido del documento ni ulterior destino que pudiera dársele. Hecha en FRANKFURT AM MAIN, ALEMANIA el día 13 del mes de febrero del año 2025.

[firma ilegible]
Nicole Marie Espaillat Vega
Vicecónsul

----------Fin del texto traducido. Firma y sello al dorso----------

Este documento se ha emitido a solicitud de parte interesada, en la ciudad de Santo Domingo, Distrito Nacional, capital de la República Dominicana, a los veintiún (21) dias del mes de febrero del año 2025.

Virginia Wall Guerra
Intérprete Judicial en los
idiomas Alemán e Inglés
(809) 754-4979

Virginia Wall Guerra
Intérprete Judicial de la República Dominicana
3/3
Alemán e Inglés

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

ZERTIFIKAT ◆ CERTIFICATE ◆ 認證證書 ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

613

Certified Copy

Management Service

CERTIFICADO

N° de registro del certificado: **12 104 54371 TMS** / N° de pedido: **707070034**

El organismo de certificación
TÜV SÜD Management Service GmbH

certifica que la organización

VERIDOS
IDENTITY SOLUTIONS

Veridos GmbH
Prinzregentenstr. 161
81677 München
Alemania

para el alcance

Diseño, desarrollo, gestión de proyectos, ventas, servicio y administración de documentos y sistemas de identificación (electrónicos)

ha implantado y aplica un sistema de gestión de medio ambiente.

Mediante auditoría realizada se verificó el cumplimiento de las exigencias recogidas en la norma

DIN EN ISO 14001:2015

Este certificado es válido del **12-07-2024** al **11-07-2027**.

CONSORCIO EMDOC

Fred Wenke
Head of Certification Body
Munich, 10-07-2024

I, Notary Public, hereby certify that this document is a true copy of the original document.

Munich, this 29.01.2025

Dr. Bernhard Schaub
Notary Public in Munich,
Federal Republic of Germany
(commission expires: October 31, 2032)

Die Echtheit vorstehender Unterschrift des Notars Dr. Bernhard Schaub und die Echtheit des beigedrückten Dienstsiegels werden hiermit bestätigt.
Zugleich wird bescheinigt, dass der Vorgenannte zur Vornahme der Amtshandlung befugt war.

München, 12. Februar 2025
Die Präsidentin des Landgerichts München I
Im Auftrag

Justizsekretärin

EMBAJADA DE LA REPÚBLICA DOMINICANA
EN ALEMANIA
SECCIÓN CONSULAR
CERTIFICO, que la firma que aparece al pie de esta documentación es la del/ de la Sr./a. Justiz-Regierungsrat
CIUDAD München y que es la misma que acostumbra a usar en todos sus actos y la cual es de su entera fé y crédito.
FECHA 14-02-2025

EMBAJADA DE LA REPÚBLICA DOMINICANA
BERLIN, ALEMANIA

HEIDI TAVERAS
CONSEJERA

CONSORCIO EMDOC
EMDOC
Santo Domingo, R.D.

6/15

EMDOC
CONSORCIO

ISO 9001:2015

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

6/6

JOSÉ MIGUEL GUERRA GONZÁLEZ

Intérprete Judicial

Yo, José Miguel Guerra González, Intérprete Judicial del Juzgado de Primera Instancia del Distrito Nacional, República Dominicana, debidamente juramentado para el ejercicio de mis funciones, CERTIFICO: Que he traducido un documento escrito en inglés y alemán cuya versión en español, a mi mejor entender, es la siguiente:

Copia Certificada

DEKRA

CERTIFICADO

MÜHLBAUER High Tech International

ISO 9001:2015

DEKRA Certification GmbH por la presente certifica que la organización

Mühlbauer ID Services GmbH

Josef-Mühlbauer-Platz 1, 93426 Roding, Alemania

para la cobertura de la certificación:

Desarrollo y distribución de soluciones completas de gobierno electrónico. Prestación de servicios de consultoría, soporte y formación en el ámbito de soluciones de gobierno electrónico. Producción de documentos de identidad, tarjetas de plástico, tarjetas inteligentes y pasaportes/pasaportes electrónicos.

(Ver ubicaciones en el anexo)

ha establecido y mantiene un sistema de gestión de calidad de acuerdo con el estándar mencionado anteriormente. El cumplimiento se registró con el informe de auditoría No. A23101492.

No. de registro del certificado:	90923503/2
Vigencia del certificado anterior:	27/05/2024
Certificado válido desde:	28/05/2024
Certificado válido hasta:	27/05/2027

Traducción

[Firmado] [Sello: DEKRA Certification GmbH - D-70565 Stuttgart Handwerkstraße 15]
Dr. Rolf Krökel
DEKRA Certification GmbH, Stuttgart, 16/05/2024

Miembro del Acuerdo Multilateral de Reconocimiento IAF

DAKKS Organismo de Acreditación de [illegible] D-ZM-16078-01-00

CONSORCIO EMDOC, Santo Domingo, RD

DEKRA

Anexo al certificado No. 90923503/2

válido del 28/05/2024 al 27/05/2027

Las siguientes ubicaciones/organizaciones pertenecen al certificado anterior:

	Sede		**Cobertura de la certificación**
	Mühlbauer ID Services GmbH	Josef-Mühlbauer-Platz 1 93426 Roding Alemania	Ver página 1
	en las siguientes ubicaciones / en las organizaciones en las siguientes ubicaciones		**Cobertura de la certificación**
1.		Manfred-von-Ardenne-Ring 15 01099 Dresde Alemania	Desarrollo de software para la captura y procesamiento de datos biométricos para documentos de identidad en el ámbito de soluciones de gobierno electrónico. Prestación de servicios de consultoría, soporte y formación en el ámbito de soluciones de gobierno electrónico.
2.		Bahnhofstraße 1-3 58095 Hagen Alemania	Desarrollo de software para la captura y procesamiento de datos biométricos para documentos de identidad en el ámbito de soluciones de gobierno electrónico. Prestación de servicios de consultoría, soporte y formación en el ámbito de soluciones de gobierno electrónico.
3.		Industriestraße 8 18069 Rostock Alemania	Desarrollo de software para la captura y procesamiento de datos biométricos para documentos de identidad en el ámbito de soluciones de gobierno electrónico. Prestación de servicios de consultoría, soporte y formación en el ámbito de soluciones de gobierno electrónico.
4.	Mühlbauer Technologies d.o.o.	Evropska 17 22300 Stara Pazova Serbia y Montenegro	Desarrollo y distribución de soluciones completas de gobierno electrónico. Prestación de servicios de consultoría, soporte y formación en el ámbito de soluciones de gobierno electrónico. Producción de documentos de identidad, tarjetas plásticas, tarjetas inteligentes y pasaportes/pasaportes electrónicos.

[Firmado] [Sello: DEKRA Certification GmbH - D-70565 Stuttgart Handwerkstraße 15]
Dr. Rolf Krökel
DEKRA Certification GmbH, Stuttgart, 16/05/2024

6/8

La copia anterior corresponde al documento original.

Roding, 19 de junio de 2024

[Firmado]
Notaria
[Sello: Katharina Marchner, Notaria de Roding]

No. de archivo 91 E 208/2024

Por este medio certifico la autenticidad de la firma que precede de la **Notaria Katharina Marchner de Roding,**

así como la autenticidad del sello oficial añadido.

Además, certifico que la persona antes mencionada está legalmente autorizada a ejecutar este acto oficial.

Ratisbona, el 19 de junio de 2024
La Presidenta del Tribunal Regional
De orden

[Firmado]
Manuela Wanner
Oficial Judicial

[Sello: Tribunal Regional de Ratisbona, Baviera]

Desglose de Costos
Impuesto: 25.00 €
(según el Art. 1, Párrafo 1 de la Ley de Costos Judiciales Estatales (LJKostG), en conjunto con la Sección 4, Párrafo 1 de la Ley de Costos de la Administración Judicial (JVKostG), KV 13.10)

El documento que antecede fue traducido en Santo Domingo, capital de la República Dominicana, el día 20 de junio del año 2024, y está registrado en mis archivos como "Certificado de Norma ISO 9001:2015 MÜHLBAUER ID SERVICES GMBH 2024072602"

JOSÉ MIGUEL GUERRA GONZÁLEZ
Intérprete Judicial
Tralega Traducciones Legales, Intérpretes Judiciales
809-535-3011 / 809-535-6011 tralega.com info@tralega.com

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

Lic. José Miguel Guerra González
INTÉRPRETE JUDICIAL DEL JUZGADO DE PRIMERA INSTANCIA D.N.
República Dominicana

6/9 Beglaubigte Abschrift

CERTIFICATE

Mühlbauer
High Tech International

ISO 9001:2015

DEKRA Certification GmbH hereby certifies that the organization

Mühlbauer ID Services GmbH

Josef-Mühlbauer-Platz 1, 93426 Roding, Germany

for the scope of certification:

Development and distribution of complete e-government solutions. Provision of consulting, support and training services in the field of e-government solutions. Production of ID documents, plastic cards, smart cards and passports/e-passports.

(Sites see annex)

has established and maintains a quality management system according to the above mentioned standard. The conformity was adduced with audit report no. A23101492.

Certificate registration no.:	909235032
Validity of previous certificate:	2024-05-27
Certificate valid from:	2024-05-28
Certificate valid to:	2027-05-27

Certification information

DEKRA

Dr. Rolf Krckel
DEKRA Certification GmbH, Stuttgart, 2024-05-16

CONSORCIO EMDOC EMDOC CONSORCIO

620

Annex to the certificate no. 90923503/2

valid from 2024-05-28 to 2027-05-27

The following sites / organizations belong to the certificate above:

	Headquarters		Scope of certification
	Mühlbauer ID Services GmbH	Josef-Mühlbauer-Platz 1 93426 Roding Germany	See page 1
	at the following sites / at the organizations at the following sites		**Scope of certification**
1.		Manfred-von-Ardenne-Ring 15 01099 Dresden Germany	Development of software for capturing and processing biometric data for ID documents in the field of e-government solutions. Provision of consulting, support and training services in the field of e-government solutions.
2.		Bahnhofstraße 1-3 58095 Hagen Germany	Development of software for capturing and processing biometric data for ID documents in the field of e-government solutions. Provision of consulting, support and training services in the field of e-government solutions.
3.		Industriestraße 15 18069 Rostock Germany	Development of software for capturing and processing biometric data for ID documents in the field of e-government solutions. Provision of consulting, support and training services in the field of e-government solutions.
4.	Mühlbauer Technologies d.o.o.	Evropska 17 22300 Stara Pazova Serbia and Montenegro	Development and distribution of complete e-government solutions. Provision of consulting, support and training services in the field of e-government solutions. Production of ID documents, plastic cards, smart cards and passports / e-passports.

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

Dr. Rolf Krökel
DEKRA Certification GmbH, Stuttgart, 2024-05-16

621

Die Ablichtung stimmt mit der Urschrift überein.
Roding, 19. JUNI 2024
Notarin

Gz. 91 E 208/2024

Die Echtheit vorstehender Unterschrift von

Notarin Katharina Marchner in Roding

und die Echtheit des beigedrückten Dienstsiegels werden hiermit bestätigt.

Zugleich wird bescheinigt, dass der/die Vorgenannte zur Vornahme der Amtshandlung gesetzlich befugt war.

Regensburg, den 19. Juni 2024
Der Präsident des Landgerichts
Im Auftrag

Manuela Wanner
Justizangestellte

BAYERN LANDGERICHT REGENSBURG

Kostenrechnung
Gebühr: 25,00 €
(gem. Art. 1 Abs. 1 JKostG, i.V.m. § 4 Abs. 1 JVKostG, KV 13 [illegible])

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

Consulado General
de la República Dominicana
en Frankfurt, Alemania

www.consuladodominicanofm@hotmail.com

622

Reg.00284/2024

CONSULADO GENERAL DE LA REPUBLICA DOMINICANA EN FRANKFURT, ALEMANIA.

CERTIFICO Y DOY FE (sin entrar en el contenido del documento ni ulterior destino que pueda dársele): que la firma que aparece al pie de **ESTA COPIA NOTARIAL**, Identificado con el **No. S/N**, de fecha **19 DE JUNIO DEL 2024,** corresponde **A LA SRA. MANUELA WANNER, PRESIDENTE DE LA AUDIENCIA PROVINCIAL**, de la ciudad de REGENSBURG, Alemania.

Y que es la Firma que acostumbra a usar en todos sus actos y a la cual se debe entera fe y crédito.

En Frankfurt am Main, Alemania, a los veintiún (21) dias del mes de junio del año dos mil veinticuatro (2024).

Niovel Aurora Tapia Ortiz
Vicecónsul

CONSULADO GENERAL DE LA REPUBLICA DOMINICANA
FRANKFURT, ALEMANIA

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

623





624

República Dominicana

MINISTERIO DE RELACIONES EXTERIORES

Viceministerio para Asuntos Consulares y Migratorios

Dirección de Legalización de Documentos

APOSTILLA

(Convention de la Haye du 5 octobre 1961)

1.País:
Country / Pays: REPÚBLICA DOMINICANA

El presente documento público
This public document / Le présent acte public

2.Ha sido firmado por:
Has been signed by / A été signé par: NIOVEL AURORA TAPIA ORTIZ

3.Quien actúa en calidad de:
Acting in the capacity of / Agissant en qualité de: VICECÓNSUL

4.Y está revestido del sello / timbre de:
Bears the seal / stamp of
Est revêtu du sceau / timbre de: CONSULADO GENERAL DE LA REPUBLICA DOMINICANA EN FRANKFURT, REPUBLICA FEDERAL DE ALEMANIA

Certificado
Certified / Attesté

5.En:
At / À: SANTO DOMINGO

6.El día:
The / Le: 28/7/2024

7.Por:
By / Par: OPINIO ANTONIO DIAZ VARGAS - VICEMINISTRO ASUNTOS CONSULARES Y MIGRATORIOS

8.Bajo el número:
N° / Sous°: AP-2024-7-28-26

9.Sello / Timbre:
Seal / Stamp
Sceau / Timbre

10.Firma:
Signature

Verificación
Verification / Vérification

País Destino:	REPÚBLICA DOMINICANA	**Código de verificación:**	KSRYVBM5EC232AB

Esta Apostilla certifica únicamente la autenticidad de la firma, la calidad en que el signatario del documento haya actuado, y en su caso, la identidad del sello o timbre del que el documento público este revestido.

This Apostille only certifies the authenticity of the signature and the capacity of the person who has signed the public document, and, where appropriate, the identity of the seal or stamp which the public document bears.

Cette Apostille atteste uniquement la véracité de la signature, la qualité en laquelle le signataire de l'acte a agi et, le cas échéant, l'identité du sceau ou timbre dont cet acte public est revêtu.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo R.D.

Certified Copy

025

Management Service

CERTIFICADO

N° de registro del certificado: **12 100 54371 TMS** / N° de pedido: **707070034**

El organismo de certificación
TÜV SÜD Management Service GmbH

certifica que la organización

VERIDOS
IDENTITY SOLUTIONS

Veridos GmbH
Prinzregentenstr. 161
81677 München
Alemania

para el alcance

Diseño, desarrollo, gestión de proyectos, ventas, servicio y administración de documentos y sistemas de identificación (electrónicos)

incluidos los emplazamientos véase el anexo

ha implantado y aplica un sistema de gestión de calidad.

Mediante auditoría realizada se verificó el cumplimiento de las exigencias recogidas en la norma

DIN EN ISO 9001:2015

Este certificado es válido del **12-07-2024** al **11-07-2027**.

Fred Wenke
Head of Certification Body
Munich, 10-07-2024

Página 1 de 2

ZERTIFIKAT ◆ CERTIFICATE ◆ 認證證書 ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT
TÜV SÜD

626

Management Service

ANEXO AL CERTIFICADO

N° de registro del certificado: **12 100 54371 TMS** / Nº de pedido: **707070034**

titular del certificado:

Veridos GmbH
Prinzregentenstr. 161
81677 München
Alemania

en los emplazamientos	alcance
Veridos GmbH Prinzregentenstr. 161 81677 München Alemania	Diseño, desarrollo, gestión de proyectos, ventas, servicio y administración de documentos y sistemas de identificación (electrónicos)
Veridos GmbH Oranienstr. 91 10969 Berlin Alemania	Venta, gestión de proyectos y administración de documentos y sistemas de identificación (electrónicos)

ZERTIFIKAT ◆ CERTIFICATE ◆ 證書 ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

Fred Wenke
Head of Certification Body
Munich, 16-07-2024

CONSORCIO EMDOC, CONSORCIO, EMDOC, Santo Domingo, R.D.

627

I, Notary Public, hereby certify that this document is a true copy of the original document.

Munich, this 29.01.2025

Dr. Bernhard Schaub
Notary Public in Munich,
Federal Republic of Germany
(commission expires: October 31, 2032)

Die Echtheit vorstehender Unterschrift des Notars Dr. Bernhard Schaub und die Echtheit des beigedrückten Dienstsiegels werden hiermit bestätigt.
Zugleich wird bescheinigt, dass der Vorgenannte zur Vornahme der Amtshandlung befugt war.

München, 07. Februar 2025
Die Präsidentin des Landgerichts München I
Im Auftrag

Lea Adelsberger
Justizsekretärin

EMBAJADA DE LA REPÚBLICA DOMINICANA
EN ALEMANIA
SECCIÓN CONSULAR
CERTIFICO, que la firma que aparece al pie de esta documentación es la del/ de la Sr./a. Adelsberger - Justizia. Regional
CIUDAD Munchen **y que es la misma que acostumbra a usar en todos sus actos y la cual es de su entera fé y crédito.**
FECHA 12-02-2025

HEIDI TAVERAS
CONSEJERA

EMBAJADA DE LA REPÚBLICA DOMINICANA EN ALEMANIA
CONSORCIO EMDOC
EMDOC CONSORCIO
Santo Domingo, R.D.

628



629

ISO 50001: 2018

CONSORCIO EMDOC
EMDOC CONSORCIO
Santo Domingo, RD

iQtek · Millbauer High Tech International · GSI · ULTRATECH · VERIDOS

Ave. 27 de febrero esquina Ave. Tiradentes. Torre Fitusa, Local 8-B
Santo Domingo, Rep. Dominicana. Tel. (809) 412-5312

Certified Copy

6630

CERTIFICATE

Mühlbauer
High Tech International

ISO 50001:2018

DEKRA Certification GmbH hereby certifies that the organization

Mühlbauer ID Services GmbH

Josef-Mühlbauer-Platz 1, 93426 Roding, Germany

for the scope of certification:

Development of hardware and software in field of e-government solutions,
provision of consulting, support and training services
in the field of e-government solutions,
provision of data center service for hardware and software development

has established and maintains an energy management system according to the above mentioned standard.
The conformity was adduced with audit report no. A23101081.

Certificate registration no.:	10092306S/1
Validity of previous certificate:	2024-08-15
Certificate valid from:	2024-09-19
Certificate valid to:	2027-08-15

DEKRA

Dr. Rolf Krokel
DEKRA Certification GmbH, Stuttgart, 2024-09-19

CONSORCIO EMDOC CONSULTORES
Santo Domingo, R.D.

631

I hereby certify that the above is a true copy of the original which has been presented to me.

Roding, 04. FEB. 2025

Katharina Marchner
notary public
(life time commission)

Ref.No. 91 E 36/2025

I hereby certify the authenticity of the above signature of the notary public

Notarin Katharina Marchner
in Roding

and the authenticity of the stamped official seal.

Furthermore, I certify that the person cited above was legally authorized of perform official duty.

Regensburg, the 07th day of February, 2025

The President of the Regional Court
by proxy

Ingrid Schwarz
Judical Administration Inspector

Cost account
Fixed charge: 25,00 €
(according to Art. 1(1) State Justice Costs Act (LJKostG) in conjunction with § 4(1) Judical Administration Costs Act (JVKostG), statement of charges 1310)

Consulado General de la República Dominicana
en Frankfurt, Alemania

Certifico: Visto bueno por legalizo la firma y el sello de INGRID SCHWARZ, PRESIDENTE DE LA AUDIENCIA PROVINCIAL, DE LA CIUDAD DE REGENSBURG, ALEMANIA., por ser, al parecer, auténtica sin prejuzgar la veracidad del contenido del documento ni alcance distinto que pueda darsele. Hecha en FRANKFURT AM MAIN, ALEMANIA. El día 13 del mes de Febrero del año 2025.

Nicole María Espaillat Vega
Vicecónsul

632

055-2025

Yo, **Virginia Wall Guerra**, Intérprete Judicial de la República Dominicana, debidamente juramentada por el Consejo del Poder Judicial, titular de la cédula de identidad y electoral número 001-1637246-7, matricula 47144, certifico que he traducido un documento cuyo original se encuentra en los idiomas INGLÉS y ALEMÁN, marcado en mi protocolo con número 055-2025, cuyo texto en el idioma ESPAÑOL se leería de la forma siguiente:

[página 1]

Copia certificada

CERTIFICADO

[logo] Mühlbauer
High Tech International

ISO 50001 : 2018

Dekra Certification GmbH certifica por este medio que la organización

Mühlbauer ID Services GmbH
Josef-Mühlbauer-Platz 1, 93426, Roding, Alemania,

para el ámbito de la certificación:

Desarrollo de hardware y software en el campo de las soluciones de gobierno electrónico. Prestación de servicios de consultoría, soporte y formación en el ámbito de las soluciones de gobierno electrónico. Proporcionar servicios de centro de datos para el desarrollo de hardware y software.

ha establecido y mantiene un sistema de gerencia de calidad de acuerdo al estándar mencionado arriba. La conformidad se adujo del informe de auditoría no. A23101081

No de registro del certificado	180923065/1
Validez del certificado anterior	2024-08-15
Certificado válido desde:	2024-09-19
Certificado válido hasta	2027-08-15

Traducción de idioma
[firma ilegible]
Dr. Rolf Krökel
DEKRA Certification GmbH, Berlin
2024-08-27

[sello redondo] *[logo]* *[logo]*
DEKRA Certification GmbH

Virginia Wall Guerra
Intérprete Judicial de la República Dominicana
113
Alemán e Inglés

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

[pie de página]
DEKRA Certification GmbH * Handwerkstraße 15* D-70565 Stuttgart * www.dekra-certification.de

633

[página 2]

[sello redondo ilegible]
KATHARINA MARCHNER
NOTARIO EN RODING

Por este medio certifico que la copia anterior es fiel a su original que fue presentado ante mí
En Roding, el 04 de febrero de 2025
[firma ilegible]
Katharina Marchner
Notario público (comisión vitalicia)

Protocolo 91 E 36/2025

Por la presente se confirma la autenticidad de la firma de la Notario **Katharina Marchner, en Roding** y la autenticidad del sello oficial adjunto.

Al mismo tiempo, se certifica que la referida persona estaba legalmente autorizada para realizar el acto oficial.

En Regensburg, el 07 de febrero de 2025
El Presidente del Tribunal Provincial
De Orden
[firma ilegible] Ingrid Schwarz
Inspectora de Administración de Justicia

[sello redondo]
BAVARIA- TRIBUNAL PROVINCIAL DE REGENSBURG

Cálculo de costos
Tasa: 25.00 euros
(de acuerdo al art. 1, párrafo 1 de la Ley de Costas Judiciales
Sección 4, párrafo 1 de la Ley de Costas Judiciales KV 13.10

Virginia Wall Guerra
Intérprete Judicial de la República Dominicana
215
Alemán e Inglés

[texto en español]

[escudo]
Consulado General de la República Dominicana
En Frankfurt, Alemania

[Código QR]
250213-235

Certifica: Visto bueno para legalizar la firma y sello de INGRID SCHWARZ, PRESIDENTE DE LA AUDIENCIA PROVINCIAL DE LA CIUDAD DE REGENSBURG, ALEMANIA., por ser, al parecer, auténtica sin prejuzgar la veracidad del contenido del documento ni ulterior destino que pudiera dársele. Hecha en FRANKFURT AM MAIN, ALEMANIA el día 13 del mes de febrero del año 2025.

CONSORCIO EMDOC
EMDOC
Santo Domingo, R.D.

[firma ilegible]
Nicole Marie Espaillat Vega
Vicecónsul

[sello redondo]
CONSULADO GENERAL DE LA REPUBLICA DOMINICANA
FRAKFURT, ALEMANIA

----------Fin del texto traducido. Firma y sello al dorso----------

634

Este documento se ha emitido a solicitud de parte interesada, en la ciudad de Santo Domingo, Distrito Nacional, capital de la República Dominicana, a los veintiún (21) días del mes de febrero del año 2025.



Virginia Wall Guerra
Intérprete Judicial en los
idiomas Alemán e Inglés
(809) 754-4979

635

EMDOC
CONSORCIO

CERTIFICADO INTERGRAF
NORMA CWA 15374:2018

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

636

JOSÉ MIGUEL GUERRA GONZÁLEZ
Intérprete Judicial

Yo, José Miguel Guerra González, Intérprete Judicial del Juzgado de Primera Instancia del Distrito Nacional, República Dominicana, debidamente juramentado para el ejercicio de mis funciones, CERTIFICO: Que he traducido un documento escrito en inglés cuya versión en español, a mi mejor entender, es la siguiente:

Copia Certificada

Certificado de INTERGRAF para Sistemas de Gestión de Seguridad para Proveedores de la Industria de Impresión de Seguridad

Intergraf por este medio certifica que, basado en los resultados de la auditoría realizada por VPGI Certification B.V., La Haya, Países Bajos, el Sistema de Gestión de Seguridad de

Proveedor de Seguridad

Mühlbauer ID Services GmbH
Josef Mühlbauer Platz 1, 93426 Roding, Alemania

cumple con los requisitos de la norma CWA 15374:2018 "Sistema de Gestión de Seguridad para Proveedores de la Industria de Impresión de Seguridad" con la cobertura siguiente:

Fabricación de equipos de producción y personalización para pasaportes electrónicos, tarjetas de identificación y otros documentos de acceso relacionados con tarjetas, así como sistemas de registro de vida y formularios y sistemas de control de acceso y fronteras totalmente automáticos, incluyendo la tecnología de hardware y software relacionada.

Número de referencia del certificado: 202303650
Fecha de expiración: 25 de mayo de 2026
Bruselas, 31 de mayo de 2023

[Sello: *Suplidor de Seguridad Certificado* - S00092]

Por Intergraf

[Firmado] [Sello: Intergraf]
Beatrice Klose
Secretaria General

Por VPGI

[Firmado] [Sello: VPGI]
Marc Been
Director General

Schleicher & Schuell Security Printing • Alemania

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

Por este medio certifico que la anterior es una copia fiel del original que ha sido presentado por ante mí.

Roding, 19 de junio de 2023

[Firmado]
Benjamin Weingarten
Notario Público
(licencia vitalicia)

[Sello: Benjamin Weingarten, Notario de Roding]

No. de archivo 91 E 201/2024

Por este medio certifico la autenticidad de la firma que precede del **Notario Benjamin Weingarten de Roding,**

así como la autenticidad del sello oficial añadido.

Además, certifico que la persona antes mencionada está legalmente autorizada a ejecutar este acto oficial.

Ratisbona, el 12 de junio de 2024
La Presidenta del Tribunal Regional
De orden

[Firmado]
Ingrid Schwarz
Inspectora de la Administración de Justicia

[Sello: Tribunal Regional de Ratisbona, Baviera]

Desglose de Costos
Impuesto: 25.00 €
(según el Art. 1, Párrafo 1 de la Ley de Costos Judiciales Estatales (LJKostG), en conjunto con la Sección 4, Párrafo 1 de la Ley de Costos de la Administración Judicial (JVKostG), KV 13.10)

El documento que antecede fue traducido en Santo Domingo, capital de la República Dominicana, el día 26 de julio del año 2024, y está registrado en mis archivos como "Certificado de Norma CWA 15374:2018 MÜNCHEN ID SERVICES GMBH 2024072601".

JOSÉ MIGUEL GUERRA GONZÁLEZ
Intérprete Judicial
Tralega Traducciones Legales, Intérpretes Judiciales
809-535-3011 / 809-535-6011 tralega.com info@tralega.com

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

Lic. José Miguel Guerra González
Intérprete Judicial del Juzgado de Primera Instancia
República Dominicana

Certified Copy

638

INTERGRAF Certificate for Security Management System for Suppliers to the Security Printing Industry

Intergraf hereby certifies that, based on the results of the audit conducted by VPGI Certification B.V., The Hague, The Netherlands, the Security Management System of

Security Supplier

Mühlbauer ID Services GmbH

Josef Mühlbauer Platz 1, 93426 Roding, Germany

complies with the requirements of the CWA 15374:2018 for "Security Management System for Supplier to the Security Printing Industry" with the scope of:

Manufacturing of production and personalization equipment for ePassports, ID cards and other card related access documents as well as life and form enrolment systems and fully automatic border and access control systems including the related hard- and software technology.

Reference Number of the Certificate: 202303650

Expiration Date: 25 May 2026

Brussels, 31 May 2023

For Intergraf

Beatrice Klose
Secretary General

INTERGRAF

For VPGI

Marc Been
Managing Director

EMDOC
CONSORCIO
Santo Domingo, R.D.

639

I hereby certify that the above
is a true copy of the original
which has been presented to me.
Roding, 19. JUNI 2023
Benjamin Weingarten
Notar
[illegible]

BENJAMIN WEINGARTEN NOTAR IN RODING

Gz. 91 E 201/2024

Die Echtheit vorstehender Unterschrift von

Notar Benjamin Weingarten
in Roding

und die Echtheit des beigedrückten Dienstsiegels
werden hiermit bestätigt.

Zugleich wird bescheinigt, dass der/die Vorgenannte
zur Vornahme der Amtshandlung gesetzlich befugt war.

Regensburg, den 12. Juni 2024
Der Präsident des Landgerichts
Im Auftrag
Ingrid Schwarz

BAYERN LANDGERICHT REGENSBURG

Ingrid Schwarz
Justizverwaltungsinspektorin

Kostenrechnung
Gebühr: 25,00 €
(gem. Art. 1 Abs. 1 LJKostG, i.V.m.
§ 4 Abs. 1 JVKostG, KV 13.10

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

Consulado General
de la República Dominicana
en Frankfurt, Alemania

Stiftstr.2, 60313 Frankfurt am Main, Alemania
Tel.:49 69 74 30 77 61 / Fax: 49 69 74 30 76 40
www.consuladodominicanoffm@hotmail.com

640

Reg.00264/2024

CONSULADO GENERAL DE LA REPUBLICA DOMINICANA EN FRANKFURT, ALEMANIA.

CERTIFICO Y DOY FE (sin entrar en el contenido del documento ni ulterior destino que pueda dársele): que la firma que aparece al pie de **ESTE CERTIFICADO**, Identificado con el **No. S/N**, de fecha **31 DE MAYO DEL 2023,** corresponde **A LA SRA. INGRID SCHWARZ**, **PRESIDENTE DE LA AUDIENCIA PROVINCIAL**, de la ciudad de REGENSBURG, Alemania.

Y que es la Firma que acostumbra a usar en todos sus actos y a la cual se debe entera fe y crédito.

En Frankfurt am Main, Alemania, a los dieciocho (18) dias del mes de junio del año dos mil veinticuatro (2024).

Niovel Aurora Tapia Ortiz
Vicecónsul

CONSULADO GENERAL DE LA REPÚBLICA DOMINICANA FRANKFURT, ALEMANIA

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

641

República Dominicana

MINISTERIO DE RELACIONES EXTERIORES

Viceministerio para Asuntos Consulares y Migratorios

Dirección de Legalización de Documentos

APOSTILLA

(Convention de la Haye du 5 octobre 1961)

1.País:
Country / Pays: REPÚBLICA DOMINICANA

El presente documento público
This public document / Le présent acte public

2.Ha sido firmado por:
Has been signed by / A été signé par: NIOVEL AURORA TAPIA ORTIZ

3.Quien actúa en calidad de:
Acting in the capacity of / Agissant en qualité de: VICECÓNSUL

4.Y está revestido del sello / timbre de:
Bears the seal / stamp of
Est revêtu du sceau / timbre de: CONSULADO GENERAL DE LA REPUBLICA DOMINICANA EN FRANKFURT, REPUBLICA FEDERAL DE ALEMANIA

Certificado
Certified / Attesté

5.En:
At / À: SANTO DOMINGO

6.El día:
The / Le: 28/7/2024

7.Por:
By / Par: OPINIO ANTONIO DIAZ VARGAS - VICEMINISTRO ASUNTOS CONSULARES Y MIGRATORIOS

8.Bajo el número:
N° / Sous°: AP-2024-7-28-13

9.Sello / Timbre:
Seal / Stamp
Sceau / Timbre

10.Firma:
Signature

Verificación
Verification / Vérification

País Destino:	REPÚBLICA DOMINICANA	**Código de verificación:**	69AJHNRG9SP29BY

Esta Apostilla certifica únicamente la autenticidad de la firma, la calidad en que el signatario del documento haya actuado, y en su caso, la identidad del sello o timbre del que el documento público está revestido.

This Apostille only certifies the authenticity of the signature and the capacity of the person who has signed the public document, and, where appropriate, the identity of the seal or stamp which the public document bears.

Cette Apostille atteste uniquement la véracité de la signature, la qualité en laquelle le signataire de l'acte a agi et, le cas échéant, l'identité du sceau ou timbre dont cet acte public est revêtu.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

642

ISO 30107

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

JOSÉ MIGUEL GUERRA GONZÁLEZ
Intérprete Judicial

Yo, José Miguel Guerra González, Intérprete Judicial del Juzgado de Primera Instancia del Distrito Nacional, República Dominicana, debidamente juramentado para el ejercicio de mis funciones, CERTIFICO: Que he traducido un documento escrito en español y alemán, cuya versión en español, a mi mejor entender, es la siguiente:

iBeta
Quality Assurance

19 de agosto de 2022

A Quien Pueda Interesar,

iBeta Quality Assurance realizó pruebas de Detección de Ataques de Presentación (PAD) de acuerdo con la norma ISO/IEC 30107-3. iBeta está acreditada por NIST/NVLAP (Código de laboratorio de pruebas NVLAP: 200962) para probar y proporcionar resultados según esta estándar de PAD (el certificado y el alcance se pueden descargar del sitio web de NVLAP).

Esta prueba se realizó con la aplicación de vida pasiva Neurotechnology Face Verification y MegaMatcher v12.1.0.0 en dos dispositivos. Ambos sistemas utilizaron el servidor de licencias "faceverification-trial-licersing-server". Las pruebas se realizaron del 9 al 19 de agosto de 2022 en un Samsung Galaxy S22 con Android 12 y una cámara web Logitech C992 Pro HD Stream en una computadora portátil con sistema operativo Windows 10.

Las pruebas se realizaron de acuerdo con el contrato para un nivel de técnica de suplantación de identidad que solo utilizaba métodos simples y fácilmente disponibles para crear artefactos biométricos genuinos para su uso en el ataque de presentación. Los sujetos de la prueba cooperaron, lo que significa que estaban dispuestos y eran capaces de proporcionar todas y cada una de las muestras biométricas, incluyendo fotografías y videos de alta calidad de su imagen. El tiempo para cada prueba de PAD por cada Instrumento de Ataque de Presentación (PAI) se limitó a ocho horas. Esto se considera un esfuerzo de prueba PAD de Nivel 1 (el primero de tres niveles).

El método de prueba fue aplicar 1 presentación de sujeto auténtica que se alternaba con 3 presentaciones de artefactos, de modo que cada especie constara de 150 ataques de presentación (PA) y 50 presentaciones auténticas. Luego, la aplicación móvil indicaría "Estado de la Operación: liveness_check_failed" para las presentaciones de artefactos y "Estado de la Operación: exitosa" para las presentaciones genuinas; la aplicación basada en Windows indicaría "Liveness Result LivenessCheckFailed" para las presentaciones de artefactos y "Livenes Result Success" para las presentaciones auténticas.

Tanto en el Galaxy S22 como en la Logitech C992 Pro, iBeta no pudo obtener una clasificación de vida con un ataque de presentación de 150 veces por especie. Con 150 Ataques de Presentación para cada una de las 6 especies en ambos dispositivos, el número total de ataques fue 1800 y la tasa de error de clasificación de presentación de ataques (APCER) fue un 0% en ambos dispositivos. También se calculó la tasa de error de clasificación de presentación genuina (BPCER) para cada dispositivo y se puede encontrar en el informe final.

iBeta probó la solución de vida pasiva Neurotechnology Face Verification y MegaMatcher v12.1.0.0 según los estándares de detección de ataques de presentación biométrica de ISO 30107-3 y cumplió con el nivel 1 en el Galaxy S22 y Logitech C992 Pro en un sistema operativo de Windows 10.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo R.D.

644

Atentamente,

[Firmado]
Ryan Borgstrom
Director de Datos Biométricos de iBeta Quality Assurance
(303) 627-1110 ext. 182
RBorgstrom@ibeta.com

2675 South Abilene Street • Suite 300 • Aurora, CO 80014 • Tel.: (303) 627-1110 • Fax (303) 627-1221

El documento que antecede fue traducido en Santo Domingo, capital de la República Dominicana, el día 26 de julio del año 2024, y está registrado en mis archivos como "Certificación iBeta 2024072601".

PROCURADURÍA GENERAL DE LA REPÚBLICA
MINISTERIO PÚBLICO
CENTRO DE ATENCIÓN AL CIUDADANO
DISTRITO NACIONAL

JOSÉ MIGUEL GUERRA GONZÁLEZ
Intérprete Judicial

INTÉRPRETE JUDICIAL DEL JUZGADO DE PRIMERA INSTANCIA DE
Lic. José Miguel Guerra González
República Dominicana

CONSORCIO EMDOC
EMDOC CONSORCIO
Santo Domingo, R.D.

6/15

iBeta
QUALITY ASSURANCE

19 August 2022

To whom it may concern,

iBeta Quality Assurance conducted Presentation Attack Detection (PAD) testing in accordance with ISO/IEC 30107-3. iBeta is accredited by NIST/NVLAP (NVLAP Testing Lab Code: 200962) to test and provide results to this PAD standard (certificate and scope may be downloaded from the NVLAP website)

This testing was conducted with the Neurotechnology Face Verification and MegaMatcher v12.1.0.0 passive liveness application on two devices. Both systems utilized the faceverification-trial-licensing-server. Testing was conducted from 9 August to 19 August 2022 on a Samsung Galaxy S22 running Android 12, and a Logitech C992 Pro HD Stream Webcam on a laptop Windows 10 system.

Testing was conducted in accordance with the contract for a level of spoofing technique that only utilized simple, readily available methods to create artefacts of the genuine biometric for use in the presentation attack. The subjects for the test effort were cooperative -- meaning that they were willing and able to provide any and all biometric samples, including high quality photos and videos of their likeness. The test time for each PAD test per PAI was limited to eight hours. This is considered a Level 1 PAD test effort (first of three levels).

The test method was to apply 1 bona fide subject presentation that alternated with 3 artefact presentations such that each species consisted of 150 Presentation Attacks (PAs) and 50 bona fide presentations. The mobile application would then state "Operation Status: livenss_check_failed" for the artefact presentations and "Operation Status: success" for bona fide presentations; the Windows-based application would state "Liveness Result LivenssCheckFailed" for the artefact presentations and "Liveness result Success" for bona fide presentations.

On both the Galaxy S22 and Logitech C992 Pro, iBeta was unable to gain a liveness classification with a presentation attack of 150 times per species. With 150 PAs for each of the 6 species on both devices, the total number of attacks was 1800 and the Attack Presentation Classification Error Rate (APCER) was 0% on both devices. The Bona Fide Presentation Classification Error Rate (BPCER) for each device was also calculated and may be found in the final report.

The Neurotechnology Face Verification and MegaMatcher v12.1.0.0 passive liveness solution was tested by iBeta to the ISO 30107-3 Biometric Presentation Attack Detection Standards and found to be in compliance with Level 1 on the Galaxy S22 and Logitech C992 Pro on a Windows 10 system.

Best regards,

Ryan Borgstrom
iBeta Quality Assurance Director of Biometrics
(303) 627-1110 ext. 182
RBorgstrom@ibeta.com

1675 South Abilene Street • Suite 300 • Aurora, CO 80014 • Phone (303) 627-1110 • Fax (303) 627-1121

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

6/6


Lita Tolksdorf
80686 München


CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo R.D.

647

Traducción certificada de la lengua alemana
de la carta de recomendación expedida en la lengua inglesa

[Logotipo de iBeta Quality Assurance]

19 de agosto de 2022

Estimados señores y señoras:

iBeta Quality Assurance realizó pruebas de detección de ataques de presentación (PAD) según la norma ISO/IEC 30107-3. iBeta está acreditada por NIST/NVLAP (código de laboratorio de pruebas NVLAP: 200962) y, por tanto, está autorizada a realizar pruebas y determinar resultados según el estándar PAD (el certificado y el alcance pueden descargarse de la página web de NVLAP).

Estas pruebas se realizaron en dos dispositivos con la aplicación «Neurotechnology Face Verification and MegaMatcher v12.1.0.0» para la detección pasiva de vida. Ambos sistemas utilizaron el servidor de licencias «faceverification-trial-licensing-server». Las pruebas se realizaron del 9 de agosto al 19 de agosto de 2022 en un Samsung Galaxy S22 con Android 12 y una cámara web Logitech C992 Pro HD Stream en un ordenador portátil con el sistema operativo Windows 10.

Las pruebas se llevaron a cabo de conformidad con el contrato para un nivel del método de ataque de suplantación de identidad en el que solo se utilizaron métodos sencillos y fácilmente disponibles para crear artefactos de los datos biométricos reales para el ataque de presentación. Los sujetos de la prueba cooperaron, es decir, estuvieron dispuestos y fueron capaces de proporcionar todas las muestras biométricas, incluidas fotos y vídeos de alta calidad de imagen. La duración de cada prueba de detección de ataques de presentación (PAD) por PA estaba limitada a ocho horas. Esto se considera una prueba PAD de nivel 1 (el primero de tres niveles).

El método de prueba consistió en utilizar una presentación de buena fe de un sujeto de prueba alternada con tres presentaciones de artefactos, de modo que se realizaron 150 ataques de presentación (PAs) y 50 presentaciones de buena fe para cada característica. En este caso, la aplicación del teléfono móvil mostraba el mensaje «Operation Status: liveness_check_failed» para las presentaciones de artefactos y «Operation Status: success» para las presentaciones de buena fe; la aplicación basada en Windows mostraba el mensaje «Liveness Result LivenessCheckFailed» para las presentaciones de artefactos y «Liveness result Success» para las presentaciones de buena fe.

Tanto en el Galaxy S22 como en el Logitech C992 Pro, iBeta fue incapaz de lograr una clasificación de detección de vida con un ataque de presentación que incluía 150 intentos por característica. Con 150 ataques de presentación para cada una de las seis características en ambos dispositivos, el número total de ataques fue de 1800 y la tasa de error de clasificación de presentación de ataque (Attack Presentation Classification Error Rate, APCER) fue del 0% en ambos dispositivos. También se calculó la tasa de error de clasificación por presentación de buena fe (Bona Fide Presentation Classification Error Rate, BPCER) para cada dispositivo, que puede consultarse en el informe final.

La solución «Neurotechnology Face Verification and MegaMatcher v12.1.0.0» para la detección pasiva de vida fue probada por iBeta de acuerdo con los estándares de reconocimiento para ataques de presentación biométrica de la norma ISO 30107-3. Corresponde al nivel 1 en el Galaxy S22 y el Logitech C992 Pro en un sistema operativo Windows 10.

Atentamente

[Firma]

Ryan Borgstrom
iBeta Quality Assurance Director of Biometrics
(303) 627-1110, Nebenstelle 182
RBorgstrom@ibeta.com
2675 South Abilene Street Suite 300 Aurora, CO 80014 TE: (303) 627-1110 Fax (303) 627-1721

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R. D.

604

Como traductora jurada de la lengua inglesa reconocida por el presidente del Tribunal regional de Múnich I, Alemania, certifico que:

La presente traducción del documento que me ha sido entregado en copia, ha sido redactado de forma correcta y completa en la lengua alemana.

Múnich, 10.06.2024

<<Sello y firma de la traductora Ute Tobiasch>>

- Fin de la traducción en lengua alemana -

Como traductora jurada de las lenguas inglesa y española reconocida por el presidente del Tribunal regional I de Múnich, Alemania, certifico que:

La presente traducción del documento que me ha sido entregado en copia, ha sido redactado de forma correcta y completa en la lengua española.

Múnich, 10.06.2024

Ute Tobiasch
Von-der-Pfordten-Str. 35
80686 München

Die Echtheit vorstehender Unterschrift der Übersetzerin Ute Tobiasch in München wird hiermit bestätigt.
Zugleich wird bescheinigt, dass die Vorgenannte öffentlich bestellte und allgemein beeidigte Übersetzerin für die französische, spanische und englische Sprache ist.

München, 12. Juni 2024
Die Präsidentin des Landgerichts München I
Im Auftrag

Markus Füssinger
Justizhauptsekretär

CONSORCIO EMDOC
EMDOC
Santo Domingo, R.D.

649

EMBAJADA DE LA REPÚBLICA DOMINICANA
EN ALEMANIA
SECCIÓN CONSULAR

CERTIFICO, que la firma que **aparece al pie de esta documentación es la del/ de la** Sr./a. Füssinger-Justicia
CIUDAD Munich **y que es la misma que acostumbra a usar en todos sus actos y la cual es de su entera fé y crédito.**
FECHA 13.06.2024

HEIDI TAVERAS
CONSEJERA

EMBAJADA DE LA REPÚBLICA DOMINICANA
BERLIN, ALEMANIA

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

650

Bestätigte Übersetzung aus der englischen Sprache

[Logo von iBeta Quality Assurance]

19. August 2022

Sehr geehrte Damen und Herren,

iBeta Quality Assurance führte Tests zur Erkennung von Präsentationsangriffen (Presentation Attack Detection, PAD) gemäß ISO/IEC 30107-3 durch. iBeta ist durch NIST/NVLAP akkreditiert (Code des NVLAP-Testlabors: 200962) und dadurch dazu berechtigt, gemäß diesem PAD-Standard Tests durchzuführen und Ergebnisse zu ermitteln (Zertifikat und Umfang können von der NVLAP-Website heruntergeladen werden).

Diese Tests wurden auf zwei Geräten mit der Anwendung „Neurotechnology Face Verification and MegaMatcher v12.1.0.0" für passive Lebenderkennung durchgeführt. Beide Systeme verwendeten den Lizenzserver „faceverification-trial-licensing-server". Die Tests wurden vom 9. August bis 19. August 2022 auf einem Samsung Galaxy S22 mit Android 12 und einer Webcam des Modells Logitech C992 Pro HD Stream auf einem Laptop mit dem Betriebssystem Windows 10 durchgeführt.

Die Tests wurden gemäß Vertrag für eine Stufe der Spoofing-Angriffsmethode durchgeführt, bei der nur einfache und problemlos verfügbare Methoden verwendet wurden, um für den Präsentationsangriff Artefakte der echten biometrischen Daten zu erstellen. Die Testpersonen verhielten sich kooperativ – das heißt, sie waren bereit und in der Lage, sämtliche biometrischen Muster bereitzustellen, einschließlich hochwertiger Fotos und Videos ihres Abbilds. Die Dauer jedes PAD-Tests pro PAI war auf acht Stunden begrenzt. Dies gilt als PAD-Testaufwand der Stufe 1 (erste von drei Stufen).

Die Testmethode bestand darin, eine Bona-fide-Präsentation einer Testperson zu verwenden, die sich mit drei Artefaktpräsentationen abwechseln sollte, sodass für jedes Merkmal 150 Präsentationsangriffe (PAs) und 50 Bona-fide-Präsentationen durchgeführt wurden. Die Anwendung auf dem Mobiltelefon zeigte in diesem Fall die Meldung „Operation Status: liveness_check_failed" für die Artefaktpräsentationen bzw. „Operation Status: success" für Bona-fide-Präsentationen an; die Windows-basierte Anwendung zeigte die Meldung „Liveness Result LivenessCheckFailed" für die Artefaktpräsentationen bzw. „Liveness result Success" für Bona-fide-Präsentationen an.

Sowohl beim Galaxy S22 als auch bei der Logitech C992 Pro konnte iBeta mit einem Präsentationsangriff, der 150 Versuche pro Merkmal umfasste, keine Lebenderkennungsklassifizierung erzielen. Mit 150 Präsentationsangriffen für jedes der sechs Merkmale auf beiden Geräten betrug die Gesamtzahl der Angriffe 1800 und die Attack Presentation Classification Error Rate (APCER) betrug auf beiden Geräten 0 %. Die Bona Fide Presentation Classification Error Rate (BPCER) für jedes Gerät wurde ebenfalls berechnet und kann dem Abschlussbericht entnommen werden.

Die Lösung „Neurotechnology Face Verification und MegaMatcher v12.1.0.0" zur passiven Lebenderkennung wurde von iBeta gemäß den Erkennungsstandards für biometrische Präsentationsangriffe der Norm ISO 30107-3 getestet. Sie entspricht auf dem Galaxy S22 und der Logitech C992 Pro auf einem Windows 10-Betriebssystem jeweils der Stufe 1.

Mit freundlichen Grüßen

[Unterschrift]

Ryan Borgstrom
iBeta Quality Assurance Director of Biometrics
(303) 627-1110, Nebenstelle 182
RBorgstrom@ibeta.com

2675 South Abilene Street Suite 300 Aurora, CO 80014 Tel: (303) 627-1130 Fax (303) 627-122

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

651

Als in Bayern öffentlich bestellte und allgemein beeidigte Übersetzerin für die englische Sprache bestätige ich:

Vorstehende Übersetzung der mir als Kopie vorgelegten, in englischer Sprache abgefassten Urkunde ist richtig und vollständig.

München, den 10.06.2024

Ute Tobiasch
Von-der-Pfordten-Str. 35
80686 München

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

652

ISO 18013-5

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

Stek Mühlbauer GSI ULTRATECH VERIDOS

Ave. 27 de Febrero esquina Rep. Dominicana, Torre Fiesta, Local 9-B
Santo Domingo, Rep. Dominicana. Tel. (809) 412-5312

fime

653

Traducción jurada del alemán

Traducción jurada del inglés

Copia notarial

Veridos
Oranienstraße 91, 10969 Berlin

2 de agosto de 2024

Asunto: Confirmación de la conformidad del VD Mobile ID basado en iOS, versión 1.0.10 (14) con la norma ISO/IEC 18013-5:2021

Estimado Sr. Nicholas:

Nos dirigimos a usted para confirmarle que la aplicación mDL mencionada anteriormente (la «aplicación») ha sido probada por FIME y ha resultado ser conforme con la norma ISO/IEC 18013-5:2021 a partir de la fecha de esta carta.

Parte de las pruebas consistió en comprobar la interfaz de la aplicación con un lector de mDL mediante la ejecución de los casos de prueba enumerados en la última versión del borrador de la norma ISO/IEC 18013-6. Solo se realizaron aquellas pruebas compatibles con las funciones de la aplicación, tal y como se especifica en la Declaración de Conformidad de la Implementación adjunta a esta carta. Para más información sobre la aplicación probada, el entorno de prueba y el equipo utilizado para la prueba, consulte la página siguiente.

Debe tenerse en cuenta que el correcto funcionamiento de la aplicación depende de diversos factores dentro de su entorno operativo. Veridos es el único y pleno responsable de la conformidad de la aplicación con todas las normas, especificaciones y requisitos aplicables.

El informe de pruebas que acompaña a esta carta lleva el número FIME_Veridos_iOS_02. Este protocolo contiene una descripción completa de los casos de prueba ejecutados y todos los resultados de las pruebas.

Atentamente
[firma ilegible]

FIME

David Bakker
Director técnico

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Do...

FIME Services North America Inc, 1945 The Exchange, Suite 200 SE, Atlanta, GA 30339, Estados Unidos

654

Ámbito de aplicación de mDL

Sistema probado

Nombre y versión de la aplicación	VO Mobile ID Versión 1.0.10 (14)
Aplicación recibida el	23 de julio de 2024

Resumen de la declaración de conformidad de la aplicación

Tecnologías para la interacción con el dispositivo	Código QR
Tecnologías para la consulta de dispositivos	BLE en el modo cliente central del Mdoc BLE en el modo servidor periférico del Mdoc
Tecnologías para la consulta del servidor	Ninguna
Mecanismos de seguridad para la consulta del dispositivo	Cifrado de las sesiones, autentificación de los datos del emisor, autentificación Mdoc ECDSA/EdDSA, autentificación de los lectores Mdoc

Entorno de prueba

Norma	ISO/IEC 18013-5:2021
Especificación de casos de prueba	Especificación de casos de prueba FIME mDL
Conjunto de pruebas	Conjunto de pruebas de la aplicación FIME mDL v1.3.14
Aplicación de prueba mDL	mdltestapp-1.3.1.apk
Dispositivo de prueba en el que está instalada la aplicación de prueba mDL	Samsung Galaxy S24
Versión del sistema operativo del dispositivo de prueba en el que está instalada la aplicación de prueba mDL	Android 14

Dispositivos de prueba y plataforma

Marca y tipo de dispositivo	iPhone 15	iPhone SE (2ª generación)
Versión del sistema operativo	iOS 17.5.1	iOS 13.5.1

655

A.1 Declaración de conformidad de la implementación

Veridos envió a la FIME las siguientes declaraciones de conformidad de la implementación (Implementation Conformance Statement, ICS). Se han utilizado para determinar los casos de prueba que deben ejecutarse.

Veridos utiliza la versión v1.10 de ICS.

A.1.1 Informaciones generales

Propietario del mDL	
Nombre del propietario de la aplicación	Veridos
Dirección	Oranienstraße 91
Ciudad	Berlin
Estado	Berlin
C.P.	10969
País	Alemania
Nombre de la persona de contacto	Nicholas Larter
Cargo	Senior Solutions Manager
Correo electrónico de la persona de contacto	nick.larter@veridos.com
Número de teléfono de la persona de contacto	+49 1525 1334198

N.º	Información general sobre la aplicación mDL	
-	Tipo de certificación	☒ Certificación de funciones[1] ☐ Certificación de producto integrado[2]
-	Nombre y versión de la aplicación	VD Mobile ID Versión 1.0.10 (14)
-	Versión iOS compatible más baja	IOS 13
	¿Cuántos documentos se pueden consultar en el mDL?	1
	Especifique el tipo de documento de cada documento	org.iso.18013.5.1. mDL
	Para cada documento, especifique todos los espacios de nombres de elementos de datos utilizados por el documento respectivo	org.iso.18013.5.1
	Para cada espacio de nombres distinto del espacio de nombres mDL («org.iso.18013.5.1»), especifique la identificación de todos los elementos de datos presentes en el documento.	

[1] Conjunto de datos del mDL para la certificación de funciones puede ser un conjunto de datos de muestra que el propietario del mDL debe proporcionar para el mDL.
[2] Para la certificación integrada de productos, el registro mDL debe ser creado y personalizado por un sistema de registro (System of Record) del emisor y debe ser representativo del mDL utilizado en la fabricación.

CONSORCIO EMDOC
EMDOC
CONSORCIO

656

A.1.2 Para los casos de prueba del modelo de datos mDL

Nota: Todos los elementos de datos de esta sección están contenidos en el espacio de nombres de datos mDL por defecto «org.iso.18013.5.1»). El ICS de esta sección sólo debe cumplimentarse para los documentos del tipo «org.iso.18013.5.1. mDL».

N.º	Declaraciones de conformidad de la implementación para los casos de prueba del modelo de datos mDL[1]	
5.	El elemento de datos administrative_number (número administrativo) está presente en los datos mDL.	☐ SÍ ☒ NO
6.	El elemento de datos sex (género) está presente en los datos mDL.	☒ SÍ ☐ NO
7.	El elemento de datos height (altura) está presente en los datos mDL.	☒ SÍ ☐ NO
8.	El elemento de datos weight (peso) está presente en los datos mDL.	☐ SÍ ☒ NO
9.	El elemento de datos eye_color (color de ojos) está presente en los datos mDL.	☒ SÍ ☐ NO
10.	El elemento de datos hair_color (color de pelo) está presente en los datos mDL.	☒ SÍ ☐ NO
11.	El elemento de datos birth_place (lugar de nacimiento) está presente en los datos mDL.	☒ SÍ ☐ NO
12.	El elemento de datos resident_address (dirección de residencia) está presente en los datos mDL.	☒ SÍ ☐ NO
13.	El elemento de datos portrait_capture_date (fecha de toma de la fotografía) está presente en los datos mDL.	☒ SÍ ☐ NO
14.	El elemento de datos age_in_years (edad en años) está presente en los datos mDL.	☒ SÍ ☐ NO
15.	El elemento de datos age_birth_year (edad año de nacimiento) está presente en los datos mDL.	☒ SÍ ☐ NO
16.	El elemento de datos age_over_NN (edad mayor que NN) está presente en los datos mDL. Si se marca SÍ: Proporcione seis (6) elementos de datos age_over_NN en los datos mDL, incluidos tres (3) valores NN inferiores con valor TRUE y tres (3) valores NN superiores con valor FALSE. Asegúrese de que el conjunto de elementos de datos age_over_NN (edad mayor que NN) sea consistente. Enumere los valores para NN1 NN6 presentes en los datos mDL.	☐ SÍ ☒ NO

Valor para NN en el identificador del	Valor (VERDADERO/FALSO)

[1] Nota: Todos los elementos de datos de esta sección están contenidos en el espacio de nombres de datos mDL estándar («org.iso.18013.5.1»). El ICS de esta sección sólo debe cumplimentarse para documentos del tipo «org.iso.18013.5.1. mDL».

CONSORCIO EMDOC EMDOC CONSORCIO

elemento de datos	
age_over_NN1(N)	VERDADERO
age_over_NN2(N)	VERDADERO
age_over_NN3(N)	VERDADERO
age_over_NN4(H)	FALSO
age_over_NN5(H)	FALSO
age_over_NN6(H)	FALSO

EJEMPLO: La frase siguiente corresponde a las reglas anteriores:

age_over_15 = VERDADERO (NN1 = 15)
age_over_18 = VERDADERO (NN2 = 18)
age_over_21 = VERDADERO (NN3 = 21)
age_over_60 = FALSO (NN4 = 60)
age_over_65 = FALSO (NN5 = 65)
age_over_68 = FALSO (NN6 = 68)

17.	El elemento de datos issuing_jurisdiction (país emisor) está disponible en los datos mDL.	☐ SÍ ☒ NO
18.	El elemento de datos nationality (nacionalidad) está disponible en los datos mDL.	☒ SÍ ☐ NO
19.	El elemento de datos resident_city (ciudad de residencia) está disponible en los datos mDL.	☒ SÍ ☐ NO
20.	El elemento de datos resident_state (estado federal de residencia) está presente en los datos mDL.	☒ SÍ ☐ NO
21.	El elemento de datos resident_postal_code (código postal del lugar de residencia) está presente en los datos mDL.	☒ SÍ ☐ NO
22.	El elemento de datos resident_country (país de residencia) está presente en los datos mDL.	☒ SÍ ☐ NO
23.	El elemento de datos biometric_template_face (plantilla biométrica de cara) está presente en los datos mDL.	☐ SÍ ☒ NO
24.	El elemento de datos biometric_template_voice (plantilla biométrica de voz) está presente en los datos mDL.	☐ SÍ ☒ NO
25.	El elemento de datos biometric_template_finger (plantilla biométrica del dedo) está presente en los datos mDL.	☐ SÍ ☒ NO
26.	El elemento de datos biometric_template_iris (plantilla biométrica del iris) está presente en los datos mDL.	☐ SÍ ☒ NO
27.	El elemento de datos biometric_template_retina (plantilla biométrica de retina) está presente en los datos mDL.	☐ SÍ ☒ NO
28.	El elemento de datos biometric_template_hand_geometry (plantilla biométrica de la geometría de la mano) está presente en los datos mDL.	☐ SÍ ☒ NO
29.	El elemento de datos biometric_template_signature_sign (plantilla biométrica de firma) está presente en los datos mDL.	☐ SÍ ☒ NO

CONSORCIO EMDOC S.A.C. EMDOC CONSORCIO

658

30.	El elemento de datos biometric_template_keystroke (plantilla biométrica de pulsación de tecla) está presente en los datos mDL.	☐ SÍ ☒ NO
31.	El elemento de datos biometric_template_lip_movement (plantilla biométrica del movimiento de los labios) está presente en los datos mDL.	☐ SÍ ☒ NO
32.	El elemento de datos biometric_template_thermal_face (plantilla biométrica facial térmica) está presente en los datos mDL.	☐ SÍ ☒ NO
33.	El elemento de datos biometric_template_thermal_hand (plantilla biométrica de mano térmica) está presente en los datos mDL.	☐ SÍ ☒ NO
34.	El elemento de datos biometric_template_gait (plantilla biométrica de la marcha) está presente en los datos mDL.	☐ SÍ ☒ NO
35.	El elemento de datos biometric_template_body_odor (plantilla biométrica del olor corporal) está presente en los datos mDL.	☐ SÍ ☒ NO
36.	El elemento de datos biometric_template_dna (plantilla biométrica de ADN) está presente en los datos mDL.	☐ SÍ ☒ NO
37.	El elemento de datos biometric_template_ear (plantilla biométrica de la oreja) está presente en los datos mDL.	☐ SÍ ☒ NO
38.	El elemento de datos biometric_template_finger_geometry (plantilla biométrica de la geometría de los dedos) está presente en los datos mDL.	☐ SÍ ☒ NO
39.	El elemento de datos biometric_template_palm_geometry (plantilla biométrica de la geometría de la palma de la mano) está presente en los datos mDL.	☐ SÍ ☒ NO
40.	El elemento de datos biometric_template_vein_pattern (plantilla biométrica del patrón de las venas) está presente en los datos mDL.	☐ SÍ ☒ NO
41.	El elemento de datos biometric_template_foot_print (plantilla biométrica de huella del pie) está presente en los datos mDL.	☐ SÍ ☒ NO
42.	El elemento de datos family_name_national_character (carácter nacional del apellido) está presente en los datos mDL.	☐ SÍ ☒ NO
43.	El elemento de datos given_name_national_character (carácter nacional del nombre) está presente en los datos mDL.	☐ SÍ ☒ NO
44.	El elemento de datos signature_usual_mark (carácter habitual de la firma) está presente en los datos mDL.	☐ SÍ ☒ NO

A.1.3 Para casos de pruebas de tecnología

N.º	Declaraciones de conformidad de la implementación para los casos de prueba de tecnología	
45.	mDL es compatible con la interacción de dispositivos mediante NFC Static Handover.	☐ SÍ ☒ NO
46.	mDL es compatible con la interacción de dispositivos vía NFC Negotiated Handover.[4]	☐ SÍ ☒ NO

[4] Nota: NFC Static Handover y NFC Negotiated Handover no se admiten simultáneamente si un mDL es compatible con ambas tecnologías.

CONSORCIO EMDOC
EMDOC
CONSORCIO

659

47.	El mDL admite la interacción de dispositivos mediante código QR.	☒ SÍ ☐ NO
48.	El mDL admite la consulta de dispositivos mediante NFC.	☐ SÍ ☒ NO
49.	El mDL admite APDUs muy largos para consulta de dispositivos mediante NFC.	☐ SÍ ☒ NO
50.	El mDl es compatible con BLE versión 4.2 (o superior) y LE Data Packet Length Extension.	☒ SÍ ☐ NO
51.	El mdL admite la consulta de dispositivos a través de BLE en el modo de cliente central del Mdoc.	☒ SÍ ☐ NO
52.	Si se utiliza BLE para la consulta de dispositivos en el modo de cliente central del Mdoc, el Mdoc verifica el valor de la característica Ident.	☐ SÍ ☒ NO
53.	El mDL admite el perfil de transmisión L2CAP cuando actúa como GATT-Client para la consulta de dispositivos a través de BLE.	☐ SÍ ☒ NO
54.	El mdL admite el sondeo de dispositivos mediante BLE en el modo de servidor periférico del Mdoc.	☒ SÍ ☐ NO
55.	El mDL admite el perfil de transmisión L2CAP cuando actúa como GATT-Server para la consulta de dispositivos mediante BLE.	☐ SÍ ☒ NO
56.	El mDL admite la consulta de dispositivos mediante Wi-Fi Aware.	☐ SÍ ☒ NO
57.	El mDL admite el conjunto de cifrado NCS-PK-2WDH-128 para Wi-Fi Aware.[5]	☐ SÍ ☒ NO
58.	El mDL admite la consulta al servidor a través de OIDC	☐ SÍ ☒ NO
59.	El mDL admite la consulta del servidor a través de WebAPI	☐ SÍ ☒ NO
60.	El mDL admite la transmisión de información de consulta al servidor dentro de la estructura de interacción del dispositivo.	☐ SÍ ☒ NO
61.	El mDL establece un tiempo de espera entre el envío de los datos de interacción con el dispositivo y la recepción del mensaje de establecimiento de sesión cuando la interacción con el dispositivo se realiza mediante código QR.	☐ SÍ ☒ NO
62.	En caso afirmativo, introduzca la duración del tiempo de espera establecido por mDL en segundos.	Ninguna
63.	El mDL establece un tiempo de espera entre el envío de los datos de interacción con el dispositivo y la recepción del mensaje de establecimiento de sesión cuando la interacción con el dispositivo se realiza mediante código NFC.	☐ SÍ ☒ NO
64.	En caso afirmativo, introduzca la duración del tiempo de espera establecido por mDL en segundos.	Ninguna

[5] Sólo se aplica si el Mdoc admite Wi-Fi Aware para el sondeo de dispositivos y NFC Negotiated Handover para la interacción de dispositivos.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo D.

660

A.1.4 Para casos de prueba de mecanismos de seguridad

N.º	Declaraciones de conformidad de la implementación para los casos de prueba de mecanismos de seguridad	
65.	¿Qué curvas admite el mDL para el establecimiento de sesión? Marque todas las curvas admitidas.[6]	☒ Curva P-256 ☐ Curva P-384 ☐ Curva P-521 ☐ X25519 ☐ X448 ☐ brainpoolP256r1 ☐ brainpoolP320r1 ☐ brainpoolP384r1 ☐ brainpoolP512r1
66.	El mDL admite el intercambio de más de una solicitud y respuesta Mdoc para la interrogación del dispositivo con el lector Mdoc en una única sesión.	☐ SÍ ☒ NO
67.	En caso afirmativo, introduzca la duración del tiempo de espera establecido por el mDL para finalizar la sesión en segundos.	
68.	¿Qué curvas admite la autoridad emisora del mDL para la autentificación de los datos del emisor? Marque todas las curvas compatibles.[7]	☒ Curva P-256 ☐ Curva P-384 ☐ Curva P-521 ☐ Ed25519 ☐ Ed448 ☐ brainpoolP256r1 ☐ brainpoolP320r1 ☐ brainpoolP384r1 ☐ brainpoolP512r1
69.	El mDL admite la autentificación Mdoc MAC.	☐ SÍ ☒ NO
70.	En caso afirmativo, ¿qué curvas admite el mDL para la autentificación Mdoc MAC? Marque todas las curvas admitidas.[8]	☐ Curva P-256 ☐ Curva P-384 ☐ Curva P-521 ☐ X25519 ☐ X448 ☐ brainpoolP256r1 ☐ brainpoolP320r1 ☐ brainpoolP384r1

[6] Si el mDL admite varias curvas de configuración de sesión, el propietario del mDL debe proporcionar una muestra de cada curva admitida para fines de prueba.

[7] Si hay varios documentos en el mDL, la autoridad emisora puede utilizar teóricamente una curva diferente para la firma MSO en cada uno de estos documentos. Sin embargo, debe tenerse en cuenta que FIME asume que se utiliza la misma curva para todos los documentos de una muestra. A efectos de prueba, el propietario del mDL deberá proporcionar una muestra para cada curva admitida.

[8] Si hay varios documentos en el mDL, el mDL puede utilizar teóricamente una curva de autenticación Mdoc MAC diferente para cada uso de [illegible]. Sin embargo, debe tenerse en cuenta que FIME asume que se utiliza la misma curva para todos los documentos de una muestra. A efectos de prueba, el propietario del mDL debe proporcionar una muestra para cada curva admitida.

CONSORCIO EMDOC
EMDOC
CONSORCIO

		☐ brainpoolP512r1
71.	El mDL admite la autentificación Mdoc ECDSA/EdDSA.	☒ SÍ ☐ NO
72.	En caso afirmativo, ¿qué curvas utiliza el mDL para la autentificación Mdoc ECDSA/EdDSA? Marque todas las curvas admitidas.[9]	☒ Curva P-256 ☐ Curva P-384 ☐ Curva P-521 ☐ Ed25519 ☐ Ed448 ☐ brainpoolP256r1 ☐ brainpoolP320r1 ☐ brainpoolP384r1 ☐ brainpoolP512r1
73.	El mDL admite la autentificación de lectores Mdoc.	☒ SÍ ☐ NO
74.	En caso afirmativo, ¿qué curvas admite el mDL para la autentificación de lectores Mdoc? Marque todas las curvas admitidas.[10]	☒ Curva P-256 ☒ Curva P-384 ☒ Curva P-521 ☐ Ed25519 ☐ Ed448 ☐ brainpoolP256r1 ☐ brainpoolP320r1 ☐ brainpoolP384r1 ☐ brainpoolP512r1
75.	En caso afirmativo, ¿notifica el Mdoc al propietario del Mdoc en caso de que falle la autentificación del lector del Mdoc de que no se ha podido verificar la identidad del comprobador?	☒ SÍ ☐ NO
76.	En caso afirmativo, ¿hay algún dato que el Mdoc no comunique en caso de que falle la autentificación del lector? Si procede, enumérelos por espacio de nombres e identificador.[11]	☐ SÍ, es decir... ☒ NO
77.	En caso afirmativo, ¿permite Mdoc la consulta de información OCSP, si está disponible, para verificar un certificado para la autentificación de lectores Mdoc?	☐ SÍ ☒ NO
78.	En caso afirmativo, ¿permite Mdoc la consulta de información CRL para verificar un certificado para la autentificación de lectores Mdoc?	☒ SÍ ☐ NO

[9] Nota: Podría haber varios pares SDeviceKey para la autenticación Mdoc para cada documento en un mDL, cada uno en un MSO separado. Por lo tanto, es teóricamente posible que un único documento utilice alternativamente autenticación MAC y autenticación ECDSA/EdDSA o que utilice alternativamente curvas diferentes para la autenticación ECDSA/EdDSA. Sin embargo, debe tenerse en cuenta que FIVE asume que el mismo método de autenticación Mdoc (MAC o [illegible]SA/EdDSA) se utiliza de forma coherente para todos los documentos de una plantilla. FIVE también asume que se utiliza la misma curva ECDSA/EdDSA para s les documentos de una muestra. A efectos de prueba, el propietario del mDL debe proporcionar una muestra para cada curva admitida.

dT asume que todos los inspectores de mDL que se nos proporcionen admiten todas las curvas invocadas para la autenticación de lectores de Mdoc (siempre que se instalen los certificados CA correctos).

[10] Al menos debe marcarse SÍ para el ref 75 o el ref 76. De lo contrario, la no autentificación de un lector no tendrá ningún efecto.

CONSORCIO EMDOC EMDOC CONSORCIO Santo

79.	Durante las pruebas, se dispone de una CRL de prueba proporcionada por el cliente para todos los certificados raíz IACA.	☐ SÍ ☒ NO
80.	Durante la prueba, está disponible una CRL de prueba para todos los certificados de firmante de documentos utilizados por el Mdoc.	☐ SÍ ☒ NO

A.1.5 Para casos de prueba de casos de aplicación

N.º	Declaraciones de conformidad de la implementación para los casos de prueba de casos de aplicación	
81.	El mDL permite que el titular del mDL deniegue el consentimiento para compartir la fotografía, pero siga consintiendo en compartir otros elementos de datos solicitados como parte de la misma solicitud.	☒ SÍ ☐ NO

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Dom...

663

Yo, representante notarial, certifico que este documento es una copia fiel del documento original.

En Múnich, a 29/01/2025

[Sello del notario]

[Firma]

Dr. Bernhard Schaub
Notario en Múnich,
República Federal de Alemania
(el mandato expira el 31 de octubre de 2032)

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo D... R.D.

664

Als in Bayern öffentlich bestellte und allgemein beeidigte Dolmetscherin für die englische und spanische Sprache bestätige ich: Vorstehende Übersetzung des mir in deutscher Sprache vorgelegten Dokuments ist richtig und vollständig.

München, den 06. Februar 2025

Como traductora jurada y nombrada públicamente para los idomas alemán, inglés y español en Baviera, confirmo que la traducción que precede del documento que se me ha presentado en lengua alemana es correcta y completa.

Münich, a 6 de febrero del 2025

Unterschrift und Stempel:

Firma y sello:

Susanne Bernhardt – Ravensburger Ring 18 – 81243 München

665

Beglaubigte Übersetzung aus dem Englischen

Notariell beglaubigte Abschrift

Veridos
Oranienstraße 91, 10969 Berlin

2. August 2024

Betreff: Bestätigung der Konformität des auf iOS basierenden VD Mobile ID, Version 1.0.10 (14) mit ISO/IEC 18013-5:2021

Sehr geehrter Herr Nicholas,

mit diesem Schreiben bestätigen wir, dass die oben genannte mDL-Anwendung (die „Anwendung") von FIME getestet und im Ergebnis festgestellt wurde, dass sie mit Stand zum Datum dieses Schreibens der Norm ISO/IEC 18013-5:2021 entspricht.

Teil des Testumfangs war die Prüfung der Anwendung auf ihre Schnittstelle zu einem mDL-Lesegerät durch Ausführung der in der neuesten Entwurfsfassung von ISO/IEC 18013-6 aufgeführten Testfälle. Die Prüfung bezog sich nur auf von der Anwendung unterstützte Funktionen, wie in der diesem Schreiben beigefügten Erklärung zur Konformität der Implementierung angegeben. Nähere Informationen zu der getesteten Anwendung, der Testumgebung und den für den Test verwendeten Prüfgeräten sind der folgenden Seite zu entnehmen.

Es wird darauf hingewiesen, dass die ordnungsgemäße Funktion der Anwendung von verschiedenen Faktoren innerhalb ihrer Betriebsumgebung abhängt. Für die Konformität der Anwendung mit allen geltenden Normen, Spezifikationen und Anforderungen trägt Veridos die alleinige und volle Verantwortung.

Das zu diesem Schreiben gehörende Prüfprotokoll trägt die Nummer FIME_Veridos_iOS_02. Dieses Protokoll enthält eine vollständige Übersicht der ausgeführten Testfälle und aller Testergebisse.

Mit freundlichen Grüßen
[unlesbare Unterschrift]

FIME

David Bakker
Technischer Leiter

CONSORCIO EMDOC
EMDOC
CONSORCIO

1

666

mDL-Implementierungsumfang

Getestetes System

Bezeichnung und Version der Anwendung	VD Mobile ID Version 1.0.10 (14)
Anwendung erhalten am	23. Juli 2024

Zusammenfassung der Erklärung zur Konformität der Implementierung

Technologien zur Geräteinteraktion	QR-Code
Technologien zur Geräteabfrage	BLE im zentralen Client-Modus des Mdoc BLE im Peripherieserver-Modus des Mdoc
Technologien zur Serverabfrage	Keine
Sicherheitsmechanismen für die Geräteabfrage	Verschlüsselung von Sitzungen, Authentifizierung von Ausstellerdaten, Mdoc ECDSA-/EdDSA-Authentifizierung, Authentifizierung von Mdoc-Lesegeräten

Testumgebung

Standard	ISO/IEC 18013-5: 2021
Testfallspezifikation	FIME mDL Testfallspezifikation
Test Suite	FIME mDL Application Test Suite v1.3.14
mDL-Testapp	mdltestapp-1.3.1.apk
Prüfgerät, auf dem die mDL-Testapp installiert ist	Samsung Galaxy S24
Version des Betriebssystems auf dem Prüfgerät, auf dem die mDL-Testapp installiert ist	Android 14

Prüfgeräte und -plattform

Marke und Typ des Geräts	iPhone 15	iPhone SE (2. Generation)
Version des Betriebssystems	iOS 17.5.1	iOS 13.5.1

CONSORCIO EMDOC
EMDOC
CONSORCIO

A.1 Erklärung zur Konformität der Implementierung

Die folgenden Erklärungen zur Konformität der Implementierung (Implementation Conformance Statement, ICS) wurden FIME von Veridos vorgelegt. Anhand dieser wurde ermittelt, welche Testfälle auszuführen sind.

Veridos verwendet die ICS-Version v1.10.

A.1.1 Allgemeine Informationen

mDL-Eigentümer	
Name des Eigentümers der Anwendung	Veridos
Adresse	Oranienstraße 91
Stadt	Berlin
Status	Berlin
PLZ	10969
Land	Deutschland
Name des Ansprechpartners	Nicholas Larter
Positionsbezeichnung	Senior Solutions Manager
E-Mail-Adresse des Ansprechpartners	nick.larter@veridos.com
Telefonnummer des Ansprechpartners	+49 1525 1334198

Nr.	Allgemeine Informationen zur mDL-Anwendung	
-	Art der Zertifizierung	☒ Funktionszertifizierung[1] ☐ Integrierte Produktzertifizierung[2]
-	Bezeichnung und Version der Anwendung	VD Mobile ID Version 1.0.10 (14)
-	Niedrigste unterstützte iOS-Version	iOS 13
	Wie viele Dokumente sind auf dem zu prüfenden mDL vorhanden?	1
	Geben Sie bitte die jeweilige Dokumentart jedes Dokuments an	org.iso.18013.5.1.mDL
	Geben Sie bitte für jedes Dokument alle vom jeweiligen Dokument verwendeten Datenelement-Namensräume an	org.iso.18013.5.1
	Geben Sie bitte für jeden vom mDL-Namensraum („org.iso.18013.5.1") abweichenden Namensraum die Bezeichner aller im Dokument vorhandenen Datenelemente an	

[1] Bei dem mDL-Datensatz für die Funktionszertifizierung kann es sich um einen Musterdatensatz handeln, den der mDL-Eigentümer mDL personalisieren möchte.
[2] Für die integrierte Produktzertifizierung muss der mDL-Datensatz von einem Aussteller-Aufzeichnungssystem (System of Record, SoR) erstellt und personalisiert werden und muss repräsentativ für den in der Herstellung verwendeten mDL sein.

CONSORCIO EMDOC EMDOC CONSORCIO

A.1.2 Für mDL-Datenmodell-Testfälle

Hinweis: Alle Datenelemente in diesem Abschnitt sind im standardmäßigen mDL-Daten-Namensraum („org.iso.18013.5.1") enthalten. Die ICS in diesem Abschnitt müssen nur für Dokumente der Dokumentart „org.iso.18013.5.1.mDL" ausgefüllt werden.

Nr.	Erklärungen zur Konformität der Implementierung für mDL-Datenmodell-Testfälle [4]	
5.	Das Datenelement administrative_number (Verwaltungsnummer) ist in den mDL-Daten vorhanden.	☐ JA ☒ NEIN
6.	Das Datenelement sex (Geschlecht) ist in den mDL-Daten vorhanden.	☒ JA ☐ NEIN
7.	Das Datenelement height (Größe) ist in den mDL-Daten vorhanden.	☒ JA ☐ NEIN
8.	Das Datenelement weight (Gewicht) ist in den mDL-Daten vorhanden.	☐ JA ☒ NEIN
9.	Das Datenelement eye_color (Augenfarbe) ist in den mDL-Daten vorhanden.	☒ JA ☐ NEIN
10.	Das Datenelement hair_color (Haarfarbe) ist in den mDL-Daten vorhanden.	☒ JA ☐ NEIN
11.	Das Datenelement birth_place (Geburtsort) ist in den mDL-Daten vorhanden.	☒ JA ☐ NEIN
12.	Das Datenelement resident_address (wohnhaft in) ist in den mDL-Daten vorhanden.	☒ JA ☐ NEIN
13.	Das Datenelement portrait_capture_date (Aufnahmedatum Lichtbild) ist in den mDL-Daten vorhanden.	☒ JA ☐ NEIN
14.	Das Datenelement age_in_years (Alter in Jahren) ist in den mDL-Daten vorhanden.	☒ JA ☐ NEIN
15.	Das Datenelement age_birth_year (Alter Geburtsjahr) ist in den mDL-Daten vorhanden.	☒ JA ☐ NEIN
16.	Das Datenelement age_over_NN (älter als NN) ist in den mDL-Daten vorhanden. Wenn JA angekreuzt wird: Bitte geben Sie sechs (6) age_over_NN Datenelemente in den mDL-Daten an, davon drei (3) niedrigere NN-Werte mit dem Wert WAHR und drei (3) höhere NN-Werte mit dem Wert FALSCH. Bitte achten Sie darauf, dass der age_over_NN Datenelemente-Satz konsistent ist. Führen Sie die in den mDL-Daten vorhandenen Werte für NN1 – NN6 auf.	☐ JA ☒ NEIN

Wert für NN in Datenelement-Bezeichner	Wert (WAHR/FALSCH)
age_over_NN1(N)	WAHR

[4] Hinweis: Alle Datenelemente in diesem Abschnitt sind im standardmäßigen mDL-Daten-Namensraum („org.iso.18013.5.1") enthalten. Die ICS in diesem Abschnitt sollen nur für Dokumente der Dokumentart „org.iso.18013.5.1.mDL" ausgefüllt werden.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo R.D.

age_over_NN2(N)	WAHR
age_over_NN3(N)	WAHR
age_over_NN4(H)	FALSCH
age_over_NN5(H)	FALSCH
age_over_NN6(H)	FALSCH

BEISPIEL: Der folgende Satz entspricht den oben angeführten Regeln:
age_over_15 = WAHR (NN1 = 15)
age_over_18 = WAHR (NN2 = 18)
age_over_21 = WAHR (NN3 = 21)
age_over_60 = FALSCH (NN4 = 60)
age_over_65 = FALSCH (NN5 = 65)
age_over_68 = FALSCH (NN6 = 68)

17.	Das Datenelement issuing_jurisdiction (Ausstellungsland) ist in den mDL-Daten vorhanden.	☐ JA ☒ NEIN
18.	Das Datenelement nationality (Nationalität) ist in den mDL-Daten vorhanden.	☒ JA ☐ NEIN
19.	Das Datenelement resident_city (Wohnort) ist in den mDL-Daten vorhanden.	☒ JA ☐ NEIN
20.	Das Datenelement resident_state (Bundesland des Wohnorts) ist in den mDL-Daten vorhanden.	☒ JA ☐ NEIN
21.	Das Datenelement resident_postal_code (PLZ des Wohnorts) ist in den mDL-Daten vorhanden.	☒ JA ☐ NEIN
22.	Das Datenelement resident_country (Land des Wohnorts) ist in den mDL-Daten vorhanden.	☒ JA ☐ NEIN
23.	Das Datenelement biometric_template_face (biometrisches Template Gesicht) ist in den mDL-Daten vorhanden.	☐ JA ☒ NEIN
24.	Das Datenelement biometric_template_voice (biometrisches Template Stimme) ist in den mDL-Daten vorhanden.	☐ JA ☒ NEIN
25.	Das Datenelement biometric_template_finger (biometrisches Template Finger) ist in den mDL-Daten vorhanden.	☐ JA ☒ NEIN
26.	Das Datenelement biometric_template_iris (biometrisches Template Iris) ist in den mDL-Daten vorhanden.	☐ JA ☒ NEIN
27.	Das Datenelement biometric_template_retina (biometrisches Template Retina) ist in den mDL-Daten vorhanden.	☐ JA ☒ NEIN
28.	Das Datenelement biometric_template_hand_geometry (biometrisches Template Handgeometrie) ist in den mDL-Daten vorhanden.	☐ JA ☒ NEIN
29.	Das Datenelement biometric_template_signature_sign (biometrisches Template Unterschrift) ist in den mDL-Daten vorhanden.	☐ JA ☒ NEIN
30.	Das Datenelement biometric_template_keystroke (biometrisches Template Tastendruck) ist in den mDL-Daten vorhanden.	☐ JA

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

31.	Das Datenelement biometric_template_lip_movement (biometrisches Template Lippenbewegung) ist in den mDL-Daten vorhanden.	☐ JA ☒ NEIN
32.	Das Datenelement biometric_template_thermal_face (biometrisches Template Gesicht, thermisch) ist in den mDL-Daten vorhanden.	☐ JA ☒ NEIN
33.	Das Datenelement biometric_template_thermal_hand (biometrisches Template Hand, thermisch) ist in den mDL-Daten vorhanden.	☐ JA ☒ NEIN
34.	Das Datenelement biometric_template_gait (biometrisches Template Gangart) ist in den mDL-Daten vorhanden.	☐ JA ☒ NEIN
35.	Das Datenelement biometric_template_body_odor (biometrisches Template Körpergeruch) ist in den mDL-Daten vorhanden.	☐ JA ☒ NEIN
36.	Das Datenelement biometric_template_dna (biometrisches Template DNS) ist in den mDL-Daten vorhanden.	☐ JA ☒ NEIN
37.	Das Datenelement biometric_template_ear (biometrisches Template Ohr) ist in den mDL-Daten vorhanden.	☐ JA ☒ NEIN
38.	Das Datenelement biometric_template_finger_geometry (biometrisches Template Fingergeometrie) ist in den mDL-Daten vorhanden.	☐ JA ☒ NEIN
39.	Das Datenelement biometric_template_palm_geometry (biometrisches Template Handinnenflächengeometrie) ist in den mDL-Daten vorhanden.	☐ JA ☒ NEIN
40.	Das Datenelement biometric_template_vein_pattern (biometrisches Template Venenmuster) ist in den mDL-Daten vorhanden.	☐ JA ☒ NEIN
41.	Das Datenelement biometric_template_foot_print (biometrisches Template Fußabdruck) ist in den mDL-Daten vorhanden.	☐ JA ☒ NEIN
42.	Das Datenelement family_name_national_character (nationale Prägung des Nachnamens) ist in den mDL-Daten vorhanden.	☐ JA ☒ NEIN
43.	Das Datenelement given_name_national_character (nationale Prägung des Vornamens) ist in den mDL-Daten vorhanden.	☐ JA ☒ NEIN
44.	Das Datenelement signature_usual_mark (übliches Zeichen in der Unterschrift) ist in den mDL-Daten vorhanden.	☐ JA ☒ NEIN

A.1.3 Für Technologie-Testfälle

Nr.	Erklärungen zur Konformität der Implementierung für Technologie-Testfälle	
45.	mDL unterstützt Geräteinteraktion über NFC Static Handover.	☐ JA ☒ NEIN
46.	mDL unterstützt Geräteinteraktion über NFC Negotiated Handover.[4]	☐ JA ☒ NEIN
47.	mDL unterstützt Geräteinteraktion über QR-Code.	☒ JA ☐ NEIN

[4] Hinweis: NFC Static Handover und NFC Negotiated Handover können nicht gleichzeitig unterstützt werden, , wenn [illegible] Technologien unterstützt.

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

48.	mDL unterstützt Geräteabfrage über NFC.	☐ JA ☒ NEIN
49.	mDL unterstützt überlange APDUs für die Geräteabfrage über NFC.	☐ JA ☒ NEIN
50.	mDl unterstützt BLE Version 4.2 (oder höher) und LE Data Packet Length Extension.	☒ JA ☐ NEIN
51.	mdL unterstützt Geräteabfrage über BLE im zentralen Client-Modus des Mdoc.	☒ JA ☐ NEIN
52.	Wird BLE im zentralen Client-Modus des Mdoc für die Geräteabfrage verwendet, verifiziert das Mdoc den Wert des Ident-Merkmals.	☐ JA ☒ NEIN
53.	mDL unterstützt das Übermittlungsprofil L2CAP, wenn es als GATT-Client für die Geräteabfrage über BLE fungiert.	☐ JA ☒ NEIN
54.	mdL unterstützt Geräteabfrage über BLE im Peripherieserver-Modus des Mdoc.	☒ JA ☐ NEIN
55.	mDL unterstützt das Übermittlungsprofil L2CAP, wenn es als GATT-Server für die Geräteabfrage über BLE fungiert.	☐ JA ☒ NEIN
56.	mDL unterstützt Geräteabfrage über Wi-Fi Aware.	☐ JA ☒ NEIN
57.	mDL unterstützt die Cipher Suite NCS-PK-2WDH-128 für Wi-Fi Aware.[5]	☐ JA ☒ NEIN
58.	mDL unterstützt Serverabfrage über DEDC	☐ JA ☒ NEIN
59.	mDL unterstützt Serverabfrage über WebAPI	☐ JA ☒ NEIN
60.	mDL unterstützt die Übermittlung von Serverabfrage-Informationen innerhalb der Geräteinteraktionsstruktur.	☐ JA ☒ NEIN
61.	mDL richtet für die Zeit zwischen dem Versand von Geräteinteraktionsdaten und dem Empfang der Mitteilung über den Aufbau der Sitzung ein Time-out ein, wenn die Geräteinteraktion über QR-Code erfolgt.	☐ JA ☒ NEIN
62.	Falls ja, geben Sie die Dauer des vom mDL eingerichteten Time-outs in Sekunden an.	keines
63.	mDL richtet für die Zeit zwischen dem Versand von Geräteinteraktionsdaten und dem Empfang der Mitteilung über den Aufbau der Sitzung ein Time-out ein, wenn die Geräteinteraktion über NFC erfolgt.	☐ JA ☒ NEIN
64.	Falls ja, geben Sie die Dauer des vom mDL eingerichteten Time-outs in Sekunden an.	Keine

[5] Gilt nur, wenn das Mdoc Wi-Fi Aware für die Geräteabfrage und NFC Negotiated Handover für die Geräteinteraktion unterstützt.

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

A.1.4 Für Sicherheitsmechanismus-Testfälle

Nr.	Erklärungen zur Konformität der Implementierung für Sicherheitsmechanismus-Testfälle	
65.	Welche Kurven unterstützt der mDL für den Aufbau von Sitzungen? Kreuzen Sie alle unterstützten Kurven an.[6]	☒ P-256 Kurve ☐ P-384 Kurve ☐ P-521 Kurve ☐ X25519 ☐ X448 ☐ brainpoolP256r1 ☐ brainpoolP320r1 ☐ brainpoolP384r1 ☐ brainpoolP512r1
66.	mDL unterstützt den Austausch von mehr als einer Mdoc-Anfrage und -Antwort zur Geräteabfrage mit dem Mdoc-Lesegerät in einer einzigen Sitzung.	☐ JA ☒ NEIN
67.	Falls ja, geben Sie die Dauer des vom mDL eingerichteten Timeouts für die Beendigung der Sitzung in Sekunden an.	
68.	Welche Kurven unterstützt die Behörde, die den mDL ausstellt, für die Authentifizierung von Ausstellerdaten? Kreuzen Sie alle unterstützten Kurven an. [7]	☒ P-256 Kurve ☐ P-384 Kurve ☐ P-521 Kurve ☐ Ed25519 ☐ Ed448 ☐ brainpoolP256r1 ☐ brainpoolP320r1 ☐ brainpoolP384r1 ☐ brainpoolP512r1
69.	mDL unterstützt Mdoc MAC-Authentifizierung.	☐ JA ☒ NEIN
70.	Falls ja, welche Kurven unterstützt der mDL für die Mdoc MAC-Authentifizierung? Kreuzen Sie alle unterstützten Kurven an.[8]	☐ P-256 Kurve ☐ P-384 Kurve ☐ P-521 Kurve ☐ X25519 ☐ X448 ☐ brainpoolP256r1

[6] Unterstützt der mDL mehrere Kurven für den Aufbau von Sitzungen, sollte der mDL-Eigentümer für Testzwecke jeweils ein Muster für jede unterstützte Kurve bereitstellen.

[7] Wenn auf dem mDL mehrere Dokumente vorhanden sind, kann die ausstellende Behörde theoretisch für die MSO-Unterzeichnung auf jedem dieser Dokumente eine andere Kurve verwenden. Es wird jedoch darauf hingewiesen, dass PIME davon ausgeht, dass für alle Dokumente in einem Muster die gleiche Kurve verwendet wird. Für Testzwecke sollte der mDL-Eigentümer jeweils ein Muster für jede unterstützte Kurve bereitstellen.

[8] Wenn auf dem mDL mehrere Dokumente vorhanden sind, kann der mDL theoretisch für jedes dieser Dokumente eine andere Authentifizierungskurve verwenden. Es wird jedoch darauf hingewiesen, dass PIME davon ausgeht, dass für alle Dokumente die gleiche Kurve verwendet wird. Für Testzwecke sollte der mDL-Eigentümer jeweils ein Muster für jede unterstützte Kurve bereitstellen.

COMERCIO EMDOC
EMDOC
Santo Domingo, R.D.

		☐ brainpoolP320r1 ☐ brainpoolP384r1 ☐ brainpoolP512r1
71.	mDL unterstützt Mdoc ECDSA-/EdDSA-Authentifizierung.	☒ JA ☐ NEIN
72.	Falls ja, welche Kurven verwendet der mDL für die Mdoc ECDSA-/EdDSA-Authentifizierung? Kreuzen Sie alle unterstützten Kurven an.[9]	☒ P-256 Kurve ☐ P-384 Kurve ☐ P-521 Kurve ☐ Ed25519 ☐ Ed448 ☐ brainpoolP256r1 ☐ brainpoolP320r1 ☐ brainpoolP384r1 ☐ brainpoolP512r1
73.	mDL unterstützt die Authentifizierung von Mdoc-Lesegeräten.	☒ JA ☐ NEIN
74.	Falls ja, welche Kurven unterstützt der mDL für die Authentifizierung von Mdoc-Lesegeräten? Kreuzen Sie alle unterstützten Kurven an. [10]	☒ P-256 Kurve ☒ P-384 Kurve ☒ P-521 Kurve ☐ Ed25519 ☐ Ed448 ☐ brainpoolP256r1 ☐ brainpoolP320r1 ☐ brainpoolP384r1 ☐ brainpoolP512r1
75.	Falls ja, benachrichtigt das Mdoc den Mdoc-Inhaber im Falle einer fehlgeschlagenen Authentifizierung des Mdoc-Lesegeräts darüber, dass die Identität des Prüfers nicht verifiziert werden konnte?	☒ JA ☐ NEIN
76.	Falls ja, gibt es Datenelemente, die das Mdoc im Falle einer fehlgeschlagenen Authentifizierung des Lesegeräts nicht freigibt? Bitte führen Sie diese ggf. anhand von Namensraum und Bezeichner auf.[11]	☐ JA, und zwar ... ☒ NEIN

[9] Hinweis: Es könnten für jedes Dokument auf einem mDL mehrere SDeviceKey-Paare für die Mdoc-Authentifizierung, jeweils in einer eigenen MSO, vorhanden sein. Daher ist es theoretisch möglich, dass ein einzelnes Dokument abwechselnd MAC-Authentifizierung und ECDSA-/EdDSA-Authentifizierung oder abwechselnd unterschiedliche Kurven für die ECDSA-/EdDSA-Authentifizierung verwendet. Es wird jedoch darauf hingewiesen, dass FIME davon ausgeht, dass für alle Dokumente in einem Muster durchgängig die gleiche Mdoc-Authentifizierungsmethode (MAC oder ECDSA/EdDSA) verwendet wird. Außerdem geht FIME davon aus, dass für alle Dokumente in einem Muster die gleiche ECDSA-/EdDSA-Kurve verwendet wird. Für Testzwecke sollte der mDL-Eigentümer jeweils ein Muster für [illegible] Kurve bereitstellen.

[10] FIME geht davon aus, dass alle uns bereitgestellten mDL-Muster alle angekreuzten Kurven für die Authentifizierung von Mdoc-Lesegeräten unterstützen (sofern die richtigen CA-Zertifikate installiert sind).

[11] Es sollte mindestens bei Nr. 75 ODER Nr. 76 JA angekreuzt werden. Andernfalls hat das Fehlschlagen der Authentifizierung [illegible] keinerlei Auswirkungen.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

77.	Falls ja, unterstützt Mdoc den Abruf von OCSP-Informationen, sofern vorhanden, zur Verifizierung eines Zertifikats für die Authentifizierung von Mdoc-Lesegeräten?	☐ JA ☒ NEIN
78.	Falls ja, unterstützt Mdoc den Abruf von CRL-Informationen zur Verifizierung eines Zertifikats für die Authentifizierung von Mdoc-Lesegeräten?	☒ JA ☐ NEIN
79.	Während der Tests steht eine vom Kunden bereitgestellte Test-CRL für alle IACA-Root-Zertifikate zur Verfügung.	☐ JA ☒ NEIN
80.	Während der Tests steht eine Test-CRL für alle vom Mdoc verwendeten Document Signer Zertifikate zur Verfügung.	☐ JA ☒ NEIN

A.1.5 Für Anwendungsfall-Testfälle

Nr.	Erklärungen zur Konformität der Implementierung für Anwendungsfall-Testfälle	
81.	Der mDL ermöglicht es dem mDL-Inhaber, seine Zustimmung zum Teilen des Lichtbilds zu verweigern, aber dennoch dem Teilen anderer im Rahmen derselben Anfrage angeforderter Datenelemente zuzustimmen.	☒ JA ☐ NEIN

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

675

Als Notar bestätige ich hiermit, dass dieses Dokument eine originalgetreue Abschrift des Originaldokuments ist.

München, den 29. Januar 2025

[Notarielles Siegel]

[Unterschrift]

Dr. Bernhard Schaub

Notar in München, Deutschland

(Kommission endet am 31. Oktober 2032)

CONSORCIO EMDOC
EMDOC
CONSORCIO

474

Als vom Präsidenten des Landgerichts München I öffentlich bestellte und allgemein beeidigte Übersetzerin für die spanische und englische Sprache bestätige ich: Vorstehende Übersetzung des mir in englischer Sprache vorgelegten Dokuments ist richtig und vollständig.

München, den 06. Februar 2025

Unterschrift und Stempel: _____

Susanne Bernhardt – Ravensburger Ring 18 – 81243 München

Die Echtheit vorstehender Unterschrift der Übersetzerin Ute Tobiasch wird hiermit bestätigt. Zugleich wird bescheinigt, dass die Vorgenannte öffentlich bestellte und allgemein beeidigte Übersetzerin für die französische, spanische Sprache ist.

München, 12. Februar 2025
Die Präsidentin des Landgerichts München I
Im Auftrag

Lea Adelsberger
Justizsekretärin

EMBAJADA DE LA REPÚBLICA DOMINICANA
EN ALEMANIA
SECCIÓN CONSULAR
CERTIFICO, que la firma que aparece al pie de esta documentación es la del/ de la Sra. Adelsberger - Justizsekretär
CIUDAD München **y que es** la misma que acostumbra a **usar en todos sus actos y la cual es de su entera fé y crédito.**
FECHA 14 - 02 - 2025

HEIDI TAVERAS
CONSEJERA

677





Certified Copy

678

fime

Veridos
Oranienstraße 91, Berlin, Germany 10969
Berlin, Germany

2nd August 2024

Subject: Confirmation of conformity of iOS-based VD Mobile ID Version 1.0.10 (14) with ISO/IEC 18013-5:2021

Dear Mr. Nicholas,

This letter serves to confirm that the abovementioned mDL application ('the application') was tested by FIME and found to be compliant with ISO/IEC 18013-5:2021 as of the date of this letter.

The test scope included testing the application on its interface to an mDL reader, by executing the test cases listed in the latest draft version of ISO/IEC 18013-6. Testing was limited to the features supported by the application, as indicated in the Implementation Conformance Statement in the Appendix to this letter. Details of the application under test, the test environment, and the test devices used for testing can be found on the next page.

As a reminder, the correct functioning of the application is dependent on several factors in its operational environment. Veridos is solely and fully responsible for the conformity of the application to all applicable standards, specifications, and requirements.

The number of the Test Report corresponding to this letter is FIME_Veridos_iOS_02. This report contains the full overview of executed test cases and all test results.

Yours sincerely,

FIME

David Bakker
Technical Lead

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

FIME Services North America Inc, 1945 The Exchange, Suite 200 SE, Atlanta, GA 30339, United States

679

mDL implementation scope

System Under Test

Application name and version	VD Mobile ID Version 1.0.10 (14)
Date of receipt of application	2024-07-23

Implementation Conformance Statement Summary

Device engagement technologies	QR code
Device retrieval technologies	BLE in mdoc central client mode BLE in mdoc peripheral server mode
Server retrieval technologies	None
Security mechanisms for device retrieval	Session encryption, issuer data authentication, mdoc ECDSA/EdDSA authentication, mdoc reader authentication

Test Environment

Standard	ISO/IEC 18013-5:2021
Test Case Specification	FIME mDL Test Case Specification
Test suite	FIME mDL Application Test Suite v1.3.14
mDL Test App	mdltestapp-1.3.1.apk
Test device on which the mDL Test App is installed	Samsung Galaxy S24
OS version of the test device on which the mDL Test App is installed	Android 14

Test Devices and Platform

Device brand and type	iPhone 15	iPhone SE (2nd Gen)
OS version	iOS 17.5.1	iOS 13.5.1

CONSORCIO EMDOC
EMDOC
CONSORCIO

680

A.1 Implementation conformance statement

The Implementation Conformance Statements below were provided to FIME by Veridos and have been used to determine which test cases to execute.

The ICS version used by Veridos is v1.10.

A.1.1 General information

mDL owner	
Application owner Name	Veridos
Address	Oranienstraße 91
City	Berlin
State	Berlin
Zip Code / Postal Code	10969
Country	Germany
Contact Name	Nicholas Larter
Contact Title	Senior Solutions Manager
Contact Email Address	nick.larter@veridos.com
Contact Phone Number	+49 1525 1334198

#	mDL Application General Information	
-	Certification Type	☒ Functional [1] ☐ Integrated Product [1]
-	Application name and version	V0 Mobile ID Version 1.0.10 (14)
-	Minimum version of IOS supported	iOS 13
	How many documents are present on the mDL under test?	1
	For each document, please specify the applicable DocType	org.iso.18013.5.1.mDL
	For each document, please specify all data element namespaces used by the document	org.iso.18013.5.1
	For each namespace different from the mDL namespace ("org.iso.18013.5.1"), please specify the identifiers of all data elements present in the document	

[1] For functional certification, the mDL data set can be a sample data set that the mDL owner would like to personalize onto the mDL.
[2] Integrated product certification requires the mDL data set to be prepared and personalized by an issuing System of Record (SoR) and the mDL data set shall be a representative of the mDL that will be used in production.
3

CONSORCIO EMDOC S.L.
EMDOC
CONSORCIO

681

A.1.2 For mdl data model test cases

Note: all the data elements in this section are in the default mDL data namespace ("org.iso.18013.5.1"). The ICS statements in this section have to be filled in only for documents having DocType = "org.iso.18013.5.1.mDL".

#	ICS statements for mDL Data Model test cases [3]	
5.	Data element administrative_number is present in the mDL data.	☐YES ☒NO
6.	Data element sex is present in the mDL data.	☒YES ☐NO
7.	Data element height is present in the mDL data.	☒YES ☐NO
8.	Data element weight is present in the mDL data.	☐YES ☒NO
9.	Data element eye_color is present in the mDL data.	☒YES ☐NO
10.	Data element hair_color is present in the mDL data.	☒YES ☐NO
11.	Data element birth_place is present in the mDL data.	☒YES ☐NO
12.	Data element resident_address is present in the mDL data.	☒YES ☐NO
13.	Data element portrait_capture_date is present in the mDL data.	☒YES ☐NO
14.	Data element age_in_years is present in the mDL data.	☒YES ☐NO
15.	Data element age_birth_year is present in the mDL data.	☒YES ☐NO
16.	Data element age_over_NN is present in the mDL data. In case you select YES, please provide six (6) age_over_NN data elements in the mDL data, of which three (3) lower NN values with the value TRUE and three (3) higher values with the value FALSE. Please make sure the set of age_over_NN data elements is consistent. List the values for NN1 – NN6 present in the mDL data.	☐YES ☒NO

[3] Note: all data elements in this section are in the default mDL data namespace ("org.iso.18013.5.1"). The ICS statements in this section should be filled in only for documents having DocType = "org.iso.18013.5.1.mDL".

CONSORCIO EMDOC
EMDOC
CONSORCIO

Value for NN in data element identifier	Value (TRUE / FALSE)
age_over_NN1(L)	TRUE
age_over_NN2(L)	TRUE
age_over_NN3(L)	TRUE
age_over_NN4(H)	FALSE
age_over_NN5(H)	FALSE
age_over_NN6(H)	FALSE

EXAMPLE: The following set complies with the above rules:

age_over_15 = TRUE	(NN1 = 15)
age_over_18 = TRUE	(NN2 = 18)
age_over_21 = TRUE	(NN3 = 21)
age_over_60 = FALSE	(NN4 = 60)
age_over_65 = FALSE	(NN5 = 65)
age_over_68 = FALSE	(NN6 = 68)

17.	Data element issuing_jurisdiction is present in the mDL data.	☐YES ☒NO
18.	Data element nationality is present in the mDL data.	☒YES ☐NO
19.	Data element resident_city is present in the mDL data.	☒YES ☐NO
20.	Data element resident_state is present in the mDL data.	☒YES ☐NO
21.	Data element resident_postal_code is present in the mDL data.	☒YES ☐NO
22.	Data element resident_country is present in the mDL data.	☒YES ☐NO
23.	Data element biometric_template_face is present in the mDL data.	☐YES ☒NO
24.	Data element biometric_template_voice is present in the mDL data.	☐YES ☒NO
25.	Data element biometric_template_finger is present in the mDL data.	☐YES ☒NO
26.	Data element biometric_template_iris is present in the mDL data.	☐YES ☒NO
27.	Data element biometric_template_retina is present in the mDL data.	☐YES ☒NO
28.	Data element biometric_template_hand_geometry is present in the mDL data.	☐YES ☒NO
29.	Data element biometric_template_signature_sign is present in the mDL data.	☐YES ☒NO

CONSORCIO EMDOC
EMDOC
CONSORCIO

30.	Data element biometric_template_keystroke is present in the mDL data.	☐YES ☒NO
31.	Data element biometric_template_lip_movement is present in the mDL data.	☐YES ☒NO
32.	Data element biometric_template_thermal_face is present in the mDL data.	☐YES ☒NO
33.	Data element biometric_template_thermal_hand is present in the mDL data.	☐YES ☒NO
34.	Data element biometric_template_gait is present in the mDL data.	☐YES ☒NO
35.	Data element biometric_template_body_odor is present in the mDL data.	☐YES ☒NO
36.	Data element biometric_template_dna is present in the mDL data.	☐YES ☒NO
37.	Data element biometric_template_ear is present in the mDL data.	☐YES ☒NO
38.	Data element biometric_template_finger_geometry is present in the mDL data.	☐YES ☒NO
39.	Data element biometric_template_palm_geometry is present in the mDL data.	☐YES ☒NO
40.	Data element biometric_template_vein_pattern is present in the mDL data.	☐YES ☒NO
41.	Data element biometric_template_foot_print is present in the mDL data.	☐YES ☒NO
42.	Data element family_name_national_character is present in the mDL data.	☐YES ☒NO
43.	Data element given_name_national_character is present in the mDL data.	☐YES ☒NO
46.	Data element signature_usual_mark is present in the mDL data.	☐YES ☒NO

A.1.3 For technology test cases

#	ICS statements for Technology test cases	
45.	mDL supports device engagement using NFC Static Handover.	☐YES ☒NO
46.	mDL supports device engagement using NFC Negotiated Handover.[4]	☐YES ☒NO

[4] Note that NFC Static Handover and NFC Negotiated Handover cannot be supported simultaneously, if an mDL supports both technologies

CONSORCIO EMDOC
EMDOC
CONSORCIO

47.	mDL supports device engagement using QR code.	☒YES ☐NO
48.	mDL supports device retrieval using NFC.	☐YES ☒NO
49.	mDL supports extended-length APDUs for device retrieval using NFC.	☐YES ☒NO
50.	mDL supports BLE version 4.2 (or above) and LE Data Packet Length Extension.	☒YES ☐NO
51.	mDL supports device retrieval using BLE in mdoc central client mode.	☒YES ☐NO
52.	If BLE in mdoc central client mode is used for device retrieval, mdoc verifies the value of the Ident characteristic.	☐YES ☒NO
53.	mDL supports the L2CAP transmission profile if it is acting as the GATT client for device retrieval using BLE.	☐YES ☒NO
54.	mDL supports device retrieval using BLE in mdoc peripheral server mode.	☒YES ☐NO
55.	mDL supports the L2CAP transmission profile if it is acting as the GATT server for device retrieval using BLE.	☐YES ☒NO
56.	mDL supports device retrieval using Wi-Fi Aware.	☐YES ☒NO
57.	mDL supports the NCS-PK-2WDH-128 cipher suite for Wi-Fi Aware.5	☐YES ☒NO
58.	mDL supports server retrieval using OIDC	☐YES ☒NO
59.	mDL supports server retrieval using WebAPI	☐YES ☒NO
60.	mDL supports transferring server retrieval information in the device engagement structure	☐YES ☒NO
61.	mDL implements a time-out for the time between sending device engagement data and receiving the session establishment message when using QR code for device engagement.	☐YES ☒NO
62.	If yes, how many seconds is the time-out period implemented by the mDL?	None
63.	mDL implements a time-out for the time between sending device engagement data and receiving the session establishment message when using NFC for device engagement.	☐YES ☒NO
64.	If yes, how many seconds is the time-out period implemented by the mDL?	None

[5] Only applicable in case the mdoc supports Wi-Fi Aware for device retrieval and supports NFC Negotiated Handover for device engagement.

CONSORCIO EMDOC
EMDOC
CONSORCIO

A.1.4 For security mechanism test cases

#	ICS statements for Security Mechanisms test cases	
65.	Which curves does the mDL support for session establishment? Select all that are supported.[6]	☒ Curve P-256 ☐ Curve P-384 ☐ Curve P-521 ☐ X25519 ☐ X448 ☐ brainpoolP256r1 ☐ brainpoolP320r1 ☐ brainpoolP384r1 ☐ brainpoolP512r1
66.	mDL supports exchanging more than one device retrieval mdoc request and response with the mdoc reader in a single session.	☐YES ☒NO
67.	If yes, how many seconds is the time-out period for session termination implemented by the mDL?	
68.	Which curves does the mDL issuing authority support for issuer data authentication? Select all that are supported.[7]	☒ Curve P-256 ☐ Curve P-384 ☐ Curve P-521 ☐ Ed25519 ☐ Ed448 ☐ brainpoolP256r1 ☐ brainpoolP320r1 ☐ brainpoolP384r1 ☐ brainpoolP512r1
69.	The mDL supports mdoc MAC authentication.	☐YES ☒NO
70.	If yes, which curves does the mDL support for mdoc MAC authentication? Select all that are supported.[8]	☐ Curve P-256 ☐ Curve P-384 ☐ Curve P-521 ☐ X25519 ☐ X448 ☐ brainpoolP256r1 ☐ brainpoolP320r1

[6] If the mDL supports multiple curves for session establishment, then for testing, the mDL owner should provide a separate sample for each of the curves supported.

[7] If multiple documents are present on the mDL, the issuing authority can in theory use a different curve for signing the MSO on each of them. However, please note that FIME expects that the same curve is used for all documents on a given sample. For testing, the mDL owner should provide a separate sample for each of the curves supported.

[8] If multiple documents are present on the mDL, the mDL can, in theory, use a different mdoc MAC authentication curve for each of them. However, please note that FIME expects that the same curve is used for all documents on a given sample. For testing, the mDL owner should provide a separate sample for each of the curves supported.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

		☐ brainpoolP384r1 ☐ brainpoolP512r1
71.	The mDL supports mdoc ECDSA/EdDSA authentication	☒ YES ☐ NO
72.	If yes, which curves does the mDL use for mdoc ECDSA/EdDSA authentication? Select all that are supported.[9]	☒ Curve P-256 ☐ Curve P-384 ☐ Curve P-521 ☐ Ed25519 ☐ Ed448 ☐ brainpoolP256r1 ☐ brainpoolP320r1 ☐ brainpoolP384r1 ☐ brainpoolP512r1
73.	The mDL supports mdoc reader authentication	☒ YES ☐ NO
74.	If yes, which curves does the mdoc support for mdoc reader authentication? Select all that are supported.[10]	☒ Curve P-256 ☒ Curve P-384 ☒ Curve P-521 ☐ Ed25519 ☐ Ed448 ☐ brainpoolP256r1 ☐ brainpoolP320r1 ☐ brainpoolP384r1 ☐ brainpoolP512r1
75.	If yes, if mdoc reader authentication fails, does the mdoc notify the mdoc holder that the mdoc verifier's identity could not be verified?	☒ YES ☐ NO
76.	If yes, are there any data elements that the mdoc will not release if reader authentication fails? If so, please list them all by namespace and identifier.[11]	☐ YES, namely… ☒ NO
77.	If yes, mdoc supports retrieving OCSP information, if available, when verifying an mdoc reader authentication certificate.	☐ YES ☒ NO

[9] Note that for each document on an mDL, there could potentially be multiple SDeviceKey pairs for mdoc authentication, each in a separate MSO. It is therefore theoretically possible that a single document uses MAC authentication and ECDSA/EdDSA authentication alternatingly or uses different curves for ECDSA/EdDSA alternatingly. However, please note that RME expects that the same mdoc authentication mechanism (either MAC or ECDSA/EdDSA) is consistently used for all documents on a given sample. Moreover, RME expects that the same ECDSA/EdDSA curve is used for all documents on a given sample. For testing, the mDL owner should provide a separate sample for each of the curves supported.

[10] RME assumes that all mDL samples provided to us will support all mdoc reader authentication curves selected (provided that the correct CA certificates are installed).

[11] At least one of ICS #75 and ICS #76 should be answered with Yes. Otherwise, failing reader authentication will not have any consequences.

CONSORCIO EMDOC
EMDOC
CONSORCIO

78.	If yes, mdoc supports retrieving CRL information when verifying a mdoc reader authentication certificate	☒YES ☐NO
79.	A test CRL for all IACA root certificates provided by the customer is available during testing.	☐YES ☒NO
80.	A test CRL for all Document Signer certificates used by the mdoc is available during testing.	☐YES ☒NO

A.1.5 For use case test cases

#	ICS statements for Use Cases test cases	
81.	The mDL enables the mDL holder to refuse consent for sharing the portrait but give consent for sharing other data elements requested in the same request.	☒YES ☐NO

CONSORCIO EMDOC
EMDOC
CONSORCIO

688

I, Notary Public, hereby certify that this document is a true copy of the original document.

Munich, this 29.01.2025

Dr. Bernhard Schaub
Notary Public in Munich,
Federal Republic of Germany
(commission expires: October 31, 2032)

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

1689


Susanne B
Ravensburger Ring 15
81243 München


CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo R.D.

fime

690

Traducción jurada del alemán

Traducción jurada del inglés

Copia notarial

Veridos
Oranienstraße 91, 10969 Berlin

2 de agosto de 2024

Asunto: Confirmación de la conformidad del Veridos Mobile ID Wallet basado en Android, versión 1.0.11, con la norma ISO/IEC 18013-5:2021

Estimado Sr. Nicholas:

Mediante la presente confirmamos que la aplicación mDL arriba mencionada (la «aplicación») ha sido probada por FIME y es conforme con la norma ISO/IEC 18013-5:2021 en la fecha de esta carta.

Parte de las pruebas consistió en comprobar la interfaz de la aplicación con un lector de mDL mediante la ejecución de los casos de prueba enumerados en la última versión del borrador de la norma ISO/IEC 18013-6. Solo se realizaron aquellas pruebas compatibles con las funciones de la aplicación, tal y como se especifica en la Declaración de Conformidad de la Implementación adjunta a esta carta. Para más información sobre la aplicación probada, el entorno de prueba y el equipo utilizado para la prueba, consulte la página siguiente.

Debe tenerse en cuenta que el correcto funcionamiento de la aplicación depende de diversos factores dentro de su entorno operativo. Veridos es el único y pleno responsable de la conformidad de la aplicación con todas las normas, especificaciones y requisitos aplicables.

El informe de pruebas que acompaña a esta carta lleva el número FIME_Veridos_Android_02. Este protocolo contiene una descripción completa de los casos de prueba ejecutados y todos los resultados de las pruebas.

Atentamente
[firma ilegible]

FIME

David Bakker
Director técnico

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

691

Ámbito de aplicación de mDL

Sistema probado

Nombre y versión de la aplicación	Veridos Mobile ID Wallet versión 1.0.11
Aplicación recibida el	23 de julio de 2024

Resumen de la declaración de conformidad de la aplicación

Tecnologías para la interacción con el dispositivo	Código QR NFC Negotiated Handover
Tecnologías para la consulta de dispositivos	BLE en el modo cliente central del Mdoc BLE en el modo servidor periférico del Mdoc
Tecnologías para la consulta del servidor	Ninguna
Mecanismos de seguridad para la consulta del dispositivo	Cifrado de las sesiones, autentificación de los datos del emisor, autentificación Mdoc ECDSA/EdDSA, autentificación de los lectores Mdoc

Entorno de prueba

Norma	ISO/IEC 18013-5: 2021
Especificación de casos de prueba	Especificación de casos de prueba FIME mDL
Conjunto de pruebas	Conjunto de pruebas de la aplicación FIME mDL v1.3.14
Aplicación de prueba mDL	mdltestapp-1.3.1.apk
Dispositivo de prueba en el que está instalada la aplicación de prueba mDL	Samsung Galaxy S20+ 5G
Versión del sistema operativo del dispositivo de prueba en el que está instalada la aplicación de prueba mDL	Android 12

Dispositivos de prueba y plataforma

Marca y tipo de dispositivo	Samsung Galaxy S24
Versión del sistema operativo	Android 14

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

692

A.1 Declaración de conformidad de la implementación

Veridos envió a la FIME las siguientes declaraciones de conformidad de la implementación (Implementation Conformance Statement, ICS). Se han utilizado para determinar los casos de prueba que deben ejecutarse.

Veridos utiliza la versión v1.10 de ICS.

A.1.1 Informaciones generales

Propietario del mDL	
Nombre del propietario de la aplicación	Veridos
Dirección	Oranienstraße 91
Ciudad	Berlín
Land	Berlín
C.P.	10969
País	Alemania
Nombre de la persona de contacto	Nicholas Larter
Cargo	Senior Solutions Manager
Correo electrónico de la persona de contacto	nick.larter@veridos.com
Número de teléfono de la persona de contacto	+49 1525 1334198

N.º	Información general sobre la aplicación mDL	
-	Tipo de certificación	☒ Certificación de funciones[1] ☐ Certificación de producto integrado[1]
-	Nombre y versión de la aplicación	Veridos Mobile ID Wallet Versión 1.0.11
-	Versión de Android compatible más baja	Android 10
	¿Cuántos documentos se pueden consultar en el mDL?	1
	Especifique el tipo de documento de cada documento	org.iso.18013.5.1. mDL
	Para cada documento, especifique todos los espacios de nombres de elementos de datos utilizados por el documento respectivo	org.iso.18013.5.1
	Para cada espacio de nombres distinto del espacio de nombres mDL («org.iso.18013.5.1»), especifique la identificación de todos los elementos de datos presentes en el documento.	

[1] El conjunto de datos del mDL para la certificación funcional puede ser un conjunto de datos de muestra que el propietario del mDL desee personalizar en el mDL. Para la certificación integrada de productos, el conjunto de datos del mDL debe ser creado y personalizado por un sistema de registro (System of Record, SoR) emisor y debe ser representativo del mDL utilizado en la fabricación.

693

A.1.2 Para los casos de prueba del modelo de datos mDL

Nota: Todos los elementos de datos de esta sección están contenidos en el espacio de nombres de datos mDL por defecto («org.iso.18013.5.1»). El ICS de esta sección sólo debe cumplimentarse para los documentos del tipo «org.iso.18013.5.1. mDL».

N.º	Declaraciones de conformidad de la implementación para los casos de prueba del modelo de datos mDL[1]	
5.	El elemento de datos administrative_number (número administrativo) está presente en los datos mDL.	☐ SÍ ☒ NO
6.	El elemento de datos sex (género) está presente en los datos mDL.	☒ SÍ ☐ NO
7.	El elemento de datos height (altura) está presente en los datos mDL.	☒ SÍ ☐ NO
8.	El elemento de datos weight (peso) está presente en los datos mDL.	☐ SÍ ☒ NO
9.	El elemento de datos eye_color (color de ojos) está presente en los datos mDL.	☒ SÍ ☐ NO
10.	El elemento de datos hair_color (color de pelo) está presente en los datos mDL.	☒ SÍ ☐ NO
11.	El elemento de datos birth_place (lugar de nacimiento) está presente en los datos mDL.	☒ SÍ ☐ NO
12.	El elemento de datos resident_address (dirección de residencia) está presente en los datos mDL.	☒ SÍ ☐ NO
13.	El elemento de datos portrait_capture_date (fecha de toma de la fotografía) está presente en los datos mDL.	☒ SÍ ☐ NO
14.	El elemento de datos age_in_years (edad en años) está presente en los datos mDL.	☒ SÍ ☐ NO
15.	El elemento de datos age_birth_year (edad fecha de nacimiento) está presente en los datos mDL.	☒ SÍ ☐ NO
16.	El elemento de datos age_over_NN (edad mayor que NN) está presente en los datos mDL. Si se marca SÍ: Proporcione seis (6) elementos de datos age_over_NN en los datos mDL, incluidos tres (3) valores NN inferiores con valor TRUE y tres (3) valores NN superiores con valor FALSE. Asegúrese de que el conjunto de elementos de datos age_over_NN sea consistente. Enumere los valores para NN1 – NN6 presentes en los datos mDL.	☐ SÍ ☒ NO

[1] Nota: Todos los elementos de datos de esta sección están contenidos en el espacio de nombres de datos mDL estándar («org.iso.18013.5.1»). El ICS de esta sección sólo debe cumplimentarse para documentos del tipo «org.iso.18013.5.1.mDL».

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

fime.c

Valor para NN en el identificador del elemento de datos	Valor (TRUE/FALSE)
age_over_NN1(N)	VERDADERO
age_over_NN2(N)	VERDADERO
age_over_NN3(N)	VERDADERO
age_over_NN4(N)	FALSO
age_over_NN5(N)	FALSO
age_over_NN6(N)	FALSO

EJEMPLO: La frase siguiente corresponde a las reglas anteriores:

age_over_15 = VERDADERO (NN1 = 15)
age_over_18 = VERDADERO (NN2 = 18)
age_over_21 = VERDADERO (NN3 = 21)
age_over_60 = FALSO (NN4 = 60)
age_over_65 = FALSO (NN5 = 65)
age_over_68 = FALSO (NN6 = 68)

17.	El elemento de datos issuing_jurisdiction (país emisor) está disponible en los datos mDL.	☐ SÍ ☒ NO
18.	El elemento de datos nationality (nacionalidad) está disponible en los datos mDL.	☒ SÍ ☐ NO
19.	El elemento de datos resident_city (ciudad de residencia) está disponible en los datos mDL.	☒ SÍ ☐ NO
20.	El elemento de datos resident_state (estado federal de residencia) está presente en los datos mDL.	☒ SÍ ☐ NO
21.	El elemento de datos resident_postal_code (código postal del lugar de residencia) está presente en los datos mDL.	☒ SÍ ☐ NO
22.	El elemento de datos resident_country (país de residencia) está presente en los datos mDL.	☒ SÍ ☐ NO
23.	El elemento de datos biometric_template_face (plantilla biométrica de cara) está presente en los datos mDL.	☐ SÍ ☒ NO
24.	El elemento de datos biometric_template_voice (plantilla biométrica de voz) está presente en los datos mDL.	☐ SÍ ☒ NO
25.	El elemento de datos biometric_template_finger (plantilla biométrica del dedo) está presente en los datos mDL.	☐ SÍ ☒ NO
26.	El elemento de datos biometric_template_iris (plantilla biométrica del iris) está presente en los datos mDL.	☐ SÍ ☒ NO
27.	El elemento de datos biometric_template_retina (plantilla biométrica de retina) está presente en los datos mDL.	☐ SÍ ☒ NO
28.	El elemento de datos biometric_template_hand_geometry (plantilla biométrica de la geometría de la mano) está presente en los datos mDL.	☐ SÍ ☒ NO

CONSORCIO EMDOC, EMDOC, CONSORCIO, Santo Domingo, R. D.

695

29.	El elemento de datos biometric_template_signature_sign (plantilla biométrica de firma) está presente en los datos mDL.	☐ SÍ ☒ NO
30.	El elemento de datos biometric_template_keystroke (plantilla biométrica de pulsación de tecla) está presente en los datos mDL.	☐ SÍ ☒ NO
31.	El elemento de datos biometric_template_lip_movement (plantilla biométrica del movimiento de los labios) está presente en los datos mDL.	☐ SÍ ☒ NO
32.	El elemento de datos biometric_template_thermal_face (plantilla biométrica facial térmica) está presente en los datos mDL.	☐ SÍ ☒ NO
33.	El elemento de datos biometric_template_thermal_hand (plantilla biométrica de mano térmica) está presente en los datos mDL.	☐ SÍ ☒ NO
34.	El elemento de datos biometric_template_gait (plantilla biométrica de la marcha) está presente en los datos mDL.	☐ SÍ ☒ NO
35.	El elemento de datos biometric_template_body_odor (plantilla biométrica de olor corporal) está presente en los datos mDL.	☐ SÍ ☒ NO
36.	El elemento de datos biometric_template_dna (plantilla biométrica de ADN) está presente en los datos mDL.	☐ SÍ ☒ NO
37.	El elemento de datos biometric_template_ear (plantilla biométrica de oreja) está presente en los datos mDL.	☐ SÍ ☒ NO
38.	El elemento de datos biometric_template_finger_geometry (plantilla biométrica de la geometría de los dedos) está presente en los datos mDL.	☐ SÍ ☒ NO
39.	El elemento de datos biometric_template_palm_geometry (plantilla biométrica de la geometría de la palma de la mano) está presente en los datos mDL.	☐ SÍ ☒ NO
40.	El elemento de datos biometric_template_vein_pattern (plantilla biométrica del patrón de venas) está presente en los datos mDL.	☐ SÍ ☒ NO
41.	El elemento de datos biometric_template_foot_print (plantilla biométrica de huella del pie) está presente en los datos mDL.	☐ SÍ ☒ NO
42.	El elemento de datos family_name_national_character (carácter nacional del apellido) está presente en los datos mDL.	☐ SÍ ☒ NO
43.	El elemento de datos given_name_national_character (carácter nacional del nombre) está presente en los datos mDL.	☐ SÍ ☒ NO
44.	El elemento de datos signature_usual_mark (carácter habitual de la firma) está presente en los datos mDL.	☐ SÍ ☒ NO

A.1.3 Para casos de pruebas de tecnología

N.º	Declaraciones de conformidad de la implementación para los casos de prueba de tecnología	
45.	El mDL es compatible con la interacción de dispositivos mediante NFC Static Handover.	☐ SÍ ☒ NO

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

46.	El mDL es compatible con la interacción de dispositivos vía NFC Negotiated Handover.[4]	☒ SÍ ☐ NO
47.	El mDL admite la interacción de dispositivos mediante código QR.	☒ SÍ ☐ NO
48.	El mDL admite la consulta de dispositivos mediante NFC.	☐ SÍ ☒ NO
49.	El mDL admite APDUs muy largos para consulta de dispositivos mediante NFC.	☐ SÍ ☒ NO
50.	El mDL es compatible con BLE versión 4.2 (o superior) y LE Data Packet Length Extension.	☒ SÍ ☐ NO
51.	El mDL admite la consulta de dispositivos a través de BLE en el modo de cliente central del Mdoc.	☒ SÍ ☐ NO
52.	Si se utiliza BLE para la consulta de dispositivos en el modo de cliente central del Mdoc, el Mdoc verifica el valor de la característica Ident.	☐ SÍ ☒ NO
53.	El mDL admite el perfil de transmisión L2CAP cuando actúa como GATT-Client para la consulta de dispositivos a través de BLE.	☐ SÍ ☒ NO
54.	El mDL admite el sondeo de dispositivos mediante BLE en el modo de servidor periférico del Mdoc.	☒ SÍ ☐ NO
55.	El mDL admite el perfil de transmisión L2CAP cuando actúa como GATT-Server para la consulta de dispositivos mediante BLE.	☐ SÍ ☒ NO
56.	El mDL admite la consulta de dispositivos mediante Wi-Fi Aware.	☐ SÍ ☒ NO
57.	El mDL admite el conjunto de cifrado NCS-PK-2WDH-128 para Wi-Fi Aware.[5]	☐ SÍ ☒ NO
58.	El mDL admite la consulta al servidor a través de OIDC	☐ SÍ ☒ NO
59.	El mDL admite la consulta del servidor a través de WebAPI	☐ SÍ ☒ NO
60.	El mDL admite la transmisión de información de consulta al servidor dentro de la estructura de interacción del dispositivo.	☐ SÍ ☒ NO
61.	El mDL establece un tiempo de espera entre el envío de los datos de interacción con el dispositivo y la recepción del mensaje de establecimiento de sesión cuando la interacción con el dispositivo se realiza mediante código QR.	☐ SÍ ☒ NO
62.	En caso afirmativo, introduzca la duración del tiempo de espera establecido por mDL en segundos.	Ninguna
63.	El mDL establece un tiempo de espera entre el envío de los datos de interacción con el dispositivo y la recepción del mensaje de establecimiento de sesión cuando la interacción con el dispositivo se realiza mediante código NFC.	☐ SÍ ☒ NO
64.	En caso afirmativo, introduzca la duración del tiempo de espera establecido por mDL en segundos.	Ninguna

[4] Nota: El traspaso estático NFC y el traspaso negociado NFC no pueden admitirse simultáneamente si un mDL es compatible con ambas tecnologías.
[5] Solo se aplica si el mdoc admite Wi-Fi Aware para el sondeo de dispositivos y NFC Negotiated Handover para la interacción de dispositivos.

CONSORCIO EMDOC
EMDOC CONSORCIO
Santo Domingo, R. D.

A.1.4 Para casos de prueba de mecanismos de seguridad

N.º	Declaraciones de conformidad de la implementación para los casos de prueba de mecanismos de seguridad	
65.	¿Qué curvas admite el mDL para el establecimiento de sesión? Marque todas las curvas admitidas.[6]	☒ Curva P-256 ☐ Curva P-384 ☐ Curva P-521 ☐ X25519 ☐ X448 ☐ brainpoolP256r1 ☐ brainpoolP320r1 ☐ brainpoolP384r1 ☐ brainpoolP512r1
66.	El mDL admite el intercambio de más de una solicitud y respuesta Mdoc para la interrogación del dispositivo con el lector Mdoc en una única sesión.	☐ Sí ☒ NO
67.	En caso afirmativo, introduzca la duración del tiempo de espera establecido por el mDL para finalizar la sesión en segundos.	
68.	¿Qué curvas admite la autoridad emisora del mDL para la autentificación de los datos del emisor? Marque todas las curvas admitidas.[7]	☒ Curva P-256 ☐ Curva P-384 ☐ Curva P-521 ☐ Ed25519 ☐ Ed448 ☐ brainpoolP256r1 ☐ brainpoolP320r1 ☐ brainpoolP384r1 ☐ brainpoolP512r1
69.	El mDL admite la autentificación Mdoc MAC.	☐ Sí ☒ NO
70.	En caso afirmativo, ¿qué curvas admite el mDL para la autentificación Mdoc MAC? Marque todas las curvas admitidas.[8]	☐ Curva P-256 ☐ Curva P-384 ☐ Curva P-521 ☐ X25519 ☐ X448 ☐ brainpoolP256r1 ☐ brainpoolP320r1

[6] Si el mDL admite varias curvas de configuración de sesión, el propietario del mDL debe proporcionar una muestra de cada curva admitida para fines de prueba.

[7] Si hay varios documentos en el mDL, la autoridad emisora puede utilizar teóricamente una curva diferente para la firma MSO en cada uno de estos documentos. Sin embargo, debe tenerse en cuenta que FIME asume que se utiliza la misma curva para todos los documentos de una muestra. A efectos de prueba, el propietario del mDL deberá proporcionar una muestra para cada curva admitida.

[8] Si hay varios documentos en el mDL, el mDL puede utilizar teóricamente una curva de autenticación Mdoc MAC diferente para cada uno de estos documentos. Sin embargo, debe tenerse en cuenta que FIME asume que se utiliza la misma curva para todos los documentos de una muestra. A efectos de prueba, el propietario del mDL debe proporcionar una muestra para cada curva admitida.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.
fime.c

		☐ brainpoolP384r1 ☐ brainpoolP512r1
71.	El mDL admite la autentificación Mdoc ECDSA/EdDSA.	☒ SÍ ☐ NO
72.	En caso afirmativo, ¿qué curvas utiliza el mDL para la autentificación Mdoc ECDSA/EdDSA? Marque todas las curvas admitidas.[9]	☒ Curva P-256 ☐ Curva P-384 ☐ Curva P-521 ☐ Ed25519 ☐ Ed448 ☐ brainpoolP256r1 ☐ brainpoolP320r1 ☐ brainpoolP384r1 ☐ brainpoolP512r1
73.	El mDL admite la autentificación de lectores Mdoc.	☒ SÍ ☐ NO
74.	En caso afirmativo, ¿qué curvas admite el mDL para la autentificación de lectores Mdoc? Marque todas las curvas admitidas.[10]	☒ Curva P-256 ☒ Curva P-384 ☒ Curva P-521 ☐ Ed25519 ☐ Ed448 ☐ brainpoolP256r1 ☐ brainpoolP320r1 ☐ brainpoolP384r1 ☐ brainpoolP512r1
75.	En caso afirmativo, ¿notifica el Mdoc al propietario del Mdoc, en caso de autentificación fallida del lector del Mdoc, que no se ha podido verificar la identidad del comprobador?	☒ SÍ ☐ NO
76.	En caso afirmativo, ¿hay algún dato que el Mdoc no comunique en caso de que falle la autentificación del lector? Enumérelos por espacio de nombres e identificador, si procede.[11]	☐ SÍ, es decir... ☒ NO
77.	En caso afirmativo, ¿permite Mdoc la consulta de información OCSP, si está disponible, para verificar un certificado para la autentificación de lectores Mdoc?	☐ SÍ ☒ NO

[9] Nota: Podría haber varios pares SDeviceKey para la autenticación Mdoc para cada documento en un mDL, cada uno en un MSO separado. Por lo tanto, es teóricamente posible que un único documento utilice alternativamente autenticación MAC y autenticación ECDSA/EdDSA o que utilice alternativamente curvas diferentes para la autenticación ECDSA/EdDSA. Sin embargo, debe tenerse en cuenta que FIME asume que el mismo método de autenticación Mdoc (MAC o ECDSA/EdDSA) se utiliza de forma coherente para todos los documentos de una plantilla. FIME también asume que se utiliza la misma curva ECDSA/EdDSA para todos los documentos de una plantilla. A nuestro. A efectos de prueba, el propietario del mDL debe proporcionar una muestra para cada curva admitida.

[10] FIME asume que todas las muestras de mDL que se nos proporcionen admiten todas las curvas marcadas para la autenticación de lectores Mdoc (siempre que se instalen los certificados CA correctos).

[11] Al menos debe marcarse SÍ para el nº 75 O el nº 76. De lo contrario, la no autentificación de un lector no tendrá ningún efecto.

CONSORCIO EMDOC, EMDOC CONSORCIO, Santo Domingo, R.D.

78.	En caso afirmativo, ¿permite Mdoc la consulta de información CRL para verificar un certificado para la autentificación de lectores Mdoc?	☒ SÍ ☐ NO
79.	Durante las pruebas, se dispone de una CRL de prueba proporcionada por el cliente para todos los certificados raíz IACA.	☐ SÍ ☒ NO
80.	Durante la prueba, está disponible una CRL de prueba para todos los certificados de firmante de documentos utilizados por el Mdoc	☐ SÍ ☒ NO

A.1.5 Para casos de prueba de casos de aplicación

7.1.5	Declaraciones de conformidad de la implementación para los casos de prueba de casos de aplicación	
81.	El mDL permite que el titular del mDL deniegue el consentimiento para compartir la fotografía, pero siga consintiendo en compartir otros elementos de datos solicitados como parte de la misma solicitud.	☒ SÍ ☐ NO

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

firma.c

700

Yo, representante notarial, certifico que este documento es una copia fiel del documento original.

En Múnich, a 29/01/2025

[Sello del notario]

[Firma]

Dr. Bernhard Schaub
Notario en Múnich,
República Federal de Alemania
(el mandato expira el 31 de octubre de 2032)

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R. D.

701

Als in Bayern öffentlich bestellte und allgemein beeidigte Dolmetscherin für die englische und spanische Sprache bestätige ich: Vorstehende Übersetzung des mir in deutscher Sprache vorgelegten Dokuments ist richtig und vollständig.

München, den 06. Februar 2025

Como traductora jurada y nombrada públicamente para los idomas alemán, inglés y español en Baviera, confirmo que la traducción que precede del documento que se me ha presentado en lengua alemana es correcta y completa.

Múnich, a 6 de febrero del 2025

Unterschrift und Stempel:

Firma y sello:

Susanne Bernhardt – Ravensburger Ring 18 – 81243 München

Die Echtheit vorstehender Unterschrift der Übersetzerin Susanne Bernhardt wird hiermit bestätigt.
Zugleich wird bescheinigt, dass die Vorgenannte öffentlich bestellte und allgemein beeidigte Übersetzerin für die spanische Sprache ist.

München, 12. Februar 2025
Die Präsidentin des Landgerichts München I
Im Auftrag

Lea Adelsberger
Justizsekretärin

fime

702

Beglaubigte Übersetzung aus dem Englischen

Notariell beglaubigte Abschrift

Veridos
Oranienstraße 91, 10969 Berlin

2. August 2024

Betreff: Bestätigung der Konformität des auf Android basierenden Veridos Mobile ID Wallet, Version 1.0.11, mit ISO/IEC 18013-5:2021

Sehr geehrter Herr Nicholas,

mit diesem Schreiben bestätigen wir, dass die oben genannte mDL-Anwendung (die „Anwendung") von FIME getestet und im Ergebnis festgestellt wurde, dass sie mit Stand zum Datum dieses Schreibens der Norm ISO/IEC 18013-5:2021 entspricht.

Teil des Testumfangs war die Prüfung der Anwendung auf ihre Schnittstelle zu einem mDL-Lesegerät durch Ausführung der in der neuesten Entwurfsfassung von ISO/IEC 18013-6 aufgeführten Testfälle. Die Prüfung bezog sich nur auf von der Anwendung unterstützte Funktionen, wie in der diesem Schreiben beigefügten Erklärung zur Konformität der Implementierung angegeben. Nähere Informationen zu der getesteten Anwendung, der Testumgebung und den für den Test verwendeten Prüfgeräten sind der folgenden Seite zu entnehmen.

Es wird darauf hingewiesen, dass die ordnungsgemäße Funktion der Anwendung von verschiedenen Faktoren innerhalb ihrer Betriebsumgebung abhängt. Für die Konformität der Anwendung mit allen geltenden Normen, Spezifikationen und Anforderungen trägt Veridos die alleinige und volle Verantwortung.

Das zu diesem Schreiben gehörende Prüfprotokoll trägt die Nummer FIME_Veridos_Android_02. Dieses Protokoll enthält eine vollständige Übersicht der ausgeführten Testfälle und aller Testergebnisse.

Mit freundlichen Grüßen
[Unlesbare Unterschrift]

FIME

David Bakker
Technischer Leiter

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

707

mDL-Implementierungsumfang

Getestetes System

Bezeichnung und Version der Anwendung	Veridos Mobile ID Wallet Version 1.0.11
Anwendung erhalten am	23. Juli 2024

Zusammenfassung der Erklärung zur Konformität der Implementierung

Technologien zur Geräteinteraktion	QR-Code NFC Negotiated Handover
Technologien zur Geräteabfrage	BLE im zentralen Client-Modus des Mdoc BLE im Peripherieserver-Modus des Mdoc
Technologien zur Serverabfrage	Keine
Sicherheitsmechanismen für die Geräteabfrage	Verschlüsselung von Sitzungen, Authentifizierung von Ausstellerdaten, Mdoc ECDSA-/EdDSA-Authentifizierung, Authentifizierung von Mdoc-Lesegeräten

Testumgebung

Standard	ISO/IEC 18013-5: 2021
Testfallspezifikation	FIME mDL Testfallspezifikation
Test Suite	FIME mDL Application Test Suite v1.3.14
mDL-Testapp	mdltestapp-1.3.1.apk
Prüfgerät, auf dem die mDL-Testapp installiert ist	Samsung Galaxy S20+ 5G
Version des Betriebssystems auf dem Prüfgerät, auf dem die mDL-Testapp installiert ist	Android 12

Prüfgeräte und -plattform

Marke und Typ des Geräts	Samsung Galaxy S24
Version des Betriebssystems	Android 14

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

A.1 Erklärung zur Konformität der Implementierung

Die folgenden Erklärungen zur Konformität der Implementierung (Implementation Conformance Statement, ICS) wurden FIME von Veridos vorgelegt. Anhand dieser wurde ermittelt, welche Testfälle auszuführen sind.

Veridos verwendet die ICS-Version v1.10.

A.1.1 Allgemeine Informationen

mDL-Eigentümer	
Name des Eigentümers der Anwendung	Veridos
Anschrift	Oranienstraße 91
Stadt	Berlin
Bundesland	Berlin
PLZ	10969
Land	Deutschland
Name des Ansprechpartners	Nicholas Larter
Positionsbezeichnung	Senior Solutions Manager
E-Mail-Adresse des Ansprechpartners	nick.larter@veridos.com
Telefonnummer des Ansprechpartners	+49 1525 1334198

Nr	Allgemeine Informationen zur mDL-Anwendung	
-	Art der Zertifizierung	☒ Funktionszertifizierung[1] ☐ Integrierte Produktzertifizierung[2]
-	Bezeichnung und Version der Anwendung	Veridos Mobile ID Wallet Version 1.0.11
-	Niedrigste unterstützte Android-Version	Android 10
	Wie viele Dokumente sind auf dem zu prüfenden mDL vorhanden?	1
	Geben Sie bitte die jeweilige Dokumentart jedes Dokuments an	org.iso.18013.5.1.mDL
	Geben Sie bitte für jedes Dokument alle vom jeweiligen Dokument verwendeten Datenelement-Namensräume an	org.iso.18013.5.1
	Geben Sie bitte für jeden vom mDL-Namensraum („org.iso.18013.5.1") abweichenden Namensraum die Bezeichner aller im Dokument vorhandenen Datenelemente an	

[1] Bei dem mDL-Datensatz für die Funktionszertifizierung kann es sich um einen Musterdatensatz handeln, den der mDL-Eigentümer [illegible] mDL personalisieren möchte.
[2] Für die integrierte Produktzertifizierung muss der mDL-Datensatz von einem Aussteller-Aufzeichnungssystem (System of Record, SoR) erstellt und personalisiert werden und muss repräsentativ für den in der Herstellung verwendeten mDL sein.

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.
fime.c

706

A.1.2 Für mDL-Datenmodell-Testfälle

Hinweis: Alle Datenelemente in diesem Abschnitt sind im standardmäßigen mDL-Daten-Namensraum („org.iso.18013.5.1") enthalten. Die ICS in diesem Abschnitt müssen nur für Dokumente der Dokumentart „org.iso.18013.5.1.mDL" ausgefüllt werden.

Nr.	Erklärungen zur Konformität der Implementierung für mDL-Datenmodell-Testfälle[1]	
5.	Das Datenelement administrative_number (Verwaltungsnummer) ist in den mDL-Daten vorhanden.	☒ JA ☒ NEIN
6.	Das Datenelement sex (Geschlecht) ist in den mDL-Daten vorhanden.	☒ JA ☐ NEIN
7.	Das Datenelement height (Größe) ist in den mDL-Daten vorhanden.	☒ JA ☐ NEIN
8.	Das Datenelement weight (Gewicht) ist in den mDL-Daten vorhanden.	☐ JA ☒ NEIN
9.	Das Datenelement eye_color (Augenfarbe) ist in den mDL-Daten vorhanden.	☒ JA ☐ NEIN
10.	Das Datenelement hair_color (Haarfarbe) ist in den mDL-Daten vorhanden.	☒ JA ☐ NEIN
11.	Das Datenelement birth_place (Geburtsort) ist in den mDL-Daten vorhanden.	☒ JA ☐ NEIN
12.	Das Datenelement resident_address (wohnhaft in) ist in den mDL-Daten vorhanden.	☒ JA ☐ NEIN
13.	Das Datenelement portrait_capture_date (Aufnahmedatum Lichtbild) ist in den mDL-Daten vorhanden.	☒ JA ☐ NEIN
14.	Das Datenelement age_in_years (Alter in Jahren) ist in den mDL-Daten vorhanden.	☒ JA ☐ NEIN
15.	Das Datenelement age_birth_year (Alter Geburtsjahr) ist in den mDL-Daten vorhanden.	☒ JA ☐ NEIN
16.	Das Datenelement age_over_NN (älter als NN) ist in den mDL-Daten vorhanden. Wenn JA angekreuzt wird: Bitte geben Sie sechs (6) age_over_NN Datenelemente in den mDL-Daten an, davon drei (3) niedrigere NN-Werte mit dem Wert WAHR und drei (3) höhere NN-Werte mit dem Wert FALSCH. Bitte achten Sie darauf, dass der age_over_NN Datenelemente-Satz konsistent ist. Führen Sie die in den mDL-Daten vorhandenen Werte für NN1 – NN6 auf.	☐ JA ☒ NEIN

[1] Hinweis: Alle Datenelemente in diesem Abschnitt sind im standardmäßigen mDL-Daten-Namensraum („org.iso.18013.5.1") enthalten. Die ICS in diesem Abschnitt müssen nur für Dokumente der Dokumentart „org.iso.18013.5.1.mDL" ausgefüllt werden.

CONSORCIO EMDOC, CONSORCIO, Santo Domingo, R.D.

fme.c

Wert für NN in Datenelement-Bezeichner	Wert (WAHR/FALSCH)
age_over_NN1(N)	WAHR
age_over_NN2(N)	WAHR
age_over_NN3(N)	WAHR
age_over_NN4(H)	FALSCH
age_over_NN5(H)	FALSCH
age_over_NN6(H)	FALSCH

BEISPIEL: Der folgende Satz entspricht den oben angeführten Regeln:

age_over_15 = WAHR (NN1 = 15)
age_over_18 = WAHR (NN2 = 18)
age_over_21 = WAHR (NN3 = 21)
age_over_60 = FALSCH (NN4 = 60)
age_over_65 = FALSCH (NN5 = 65)
age_over_68 = FALSCH (NN6 = 68)

17.	Das Datenelement issuing_jurisdiction (Ausstellungsland) ist in den mDL-Daten vorhanden.	☐ JA ☒ NEIN
18.	Das Datenelement nationality (Nationalität) ist in den mDL-Daten vorhanden.	☒ JA ☐ NEIN
19.	Das Datenelement resident_city (Wohnort) ist in den mDL-Daten vorhanden.	☒ JA ☐ NEIN
20.	Das Datenelement resident_state (Bundesland des Wohnorts) ist in den mDL-Daten vorhanden.	☒ JA ☐ NEIN
21.	Das Datenelement resident_postal_code (PLZ des Wohnorts) ist in den mDL-Daten vorhanden.	☒ JA ☐ NEIN
22.	Das Datenelement resident_country (Land des Wohnorts) ist in den mDL-Daten vorhanden.	☒ JA ☐ NEIN
23.	Das Datenelement biometric_template_face (biometrisches Template Gesicht) ist in den mDL-Daten vorhanden.	☐ JA ☒ NEIN
24.	Das Datenelement biometric_template_voice (biometrisches Template Stimme) ist in den mDL-Daten vorhanden.	☐ JA ☒ NEIN
25.	Das Datenelement biometric_template_finger (biometrisches Template Finger) ist in den mDL-Daten vorhanden.	☐ JA ☒ NEIN
26.	Das Datenelement biometric_template_iris (biometrisches Template Iris) ist in den mDL-Daten vorhanden.	☐ JA ☒ NEIN
27.	Das Datenelement biometric_template_retina (biometrisches Template Retina) ist in den mDL-Daten vorhanden.	☐ JA ☒ NEIN
28.	Das Datenelement biometric_template_hand_geometry (biometrisches Template Handgeometrie) ist in den mDL-Daten vorhanden.	☐ JA ☒ NEIN

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

fme.c

29.	Das Datenelement biometric_template_signature_sign (biometrisches Template Unterschrift) ist in den mDL-Daten vorhanden.	☐ JA ☒ NEIN
30.	Das Datenelement biometric_template_keystroke (biometrisches Template Tastendruck) ist in den mDL-Daten vorhanden.	☐ JA ☒ NEIN
31.	Das Datenelement biometric_template_lip_movement (biometrisches Template Lippenbewegung) ist in den mDL-Daten vorhanden.	☐ JA ☒ NEIN
32.	Das Datenelement biometric_template_thermal_face (biometrisches Template Gesicht, thermisch) ist in den mDL-Daten vorhanden.	☐ JA ☒ NEIN
33.	Das Datenelement biometric_template_thermal_hand (biometrisches Template Hand, thermisch) ist in den mDL-Daten vorhanden.	☐ JA ☒ NEIN
34.	Das Datenelement biometric_template_gait (biometrisches Template Gangart) ist in den mDL-Daten vorhanden.	☐ JA ☒ NEIN
35.	Das Datenelement biometric_template_body_odor (biometrisches Template Körpergeruch) ist in den mDL-Daten vorhanden.	☐ JA ☒ NEIN
36.	Das Datenelement biometric_template_dna (biometrisches Template DNS) ist in den mDL-Daten vorhanden.	☐ JA ☒ NEIN
37.	Das Datenelement biometric_template_ear (biometrisches Template Ohr) ist in den mDL-Daten vorhanden.	☐ JA ☒ NEIN
38.	Das Datenelement biometric_template_finger_geometry (biometrisches Template Fingergeometrie) ist in den mDL-Daten vorhanden.	☐ JA ☒ NEIN
39.	Das Datenelement biometric_template_palm_geometry (biometrisches Template Handinnenflächengeometrie) ist in den mDL-Daten vorhanden.	☐ JA ☒ NEIN
40.	Das Datenelement biometric_template_vein_pattern (biometrisches Template Venenmuster) ist in den mDL-Daten vorhanden.	☐ JA ☒ NEIN
41.	Das Datenelement biometric_template_foot_print (biometrisches Template Fußabdruck) ist in den mDL-Daten vorhanden.	☐ JA ☒ NEIN
42.	Das Datenelement family_name_national_character (nationale Prägung des Nachnamens) ist in den mDL-Daten vorhanden.	☐ JA ☒ NEIN
43.	Das Datenelement given_name_national_character (nationale Prägung des Vornamens) ist in den mDL-Daten vorhanden.	☐ JA ☒ NEIN
44.	Das Datenelement signature_usual_mark (übliches Zeichen in der Unterschrift) ist in den mDL-Daten vorhanden.	☐ JA ☒ NEIN

A.1.3 Für Technologie-Testfälle

Nr.	Erklärungen zur Konformität der Implementierung für Technologie-Testfälle	
45.	mDL unterstützt Geräteinteraktion über NFC Static Handover.	☐ JA ☒ NEIN

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R. D.

46.	mDL unterstützt Geräteinteraktion über NFC Negotiated Handover[4].	☒ JA ☐ NEIN
47.	mDL unterstützt Geräteinteraktion über QR-Code.	☒ JA ☐ NEIN
48.	mDL unterstützt Geräteabfrage über NFC.	☐ JA ☒ NEIN
49.	mDL unterstützt überlange APDUs für die Geräteabfrage über NFC.	☐ JA ☒ NEIN
50.	mDL unterstützt BLE Version 4.2 (oder höher) und LE Data Packet Length Extension.	☒ JA ☐ NEIN
51.	mDL unterstützt Geräteabfrage über BLE im zentralen Client-Modus des Mdoc.	☒ JA ☐ NEIN
52.	Wird BLE im zentralen Client-Modus des Mdoc für die Geräteabfrage verwendet, verifiziert das Mdoc den Wert des Ident-Merkmals.	☐ JA ☒ NEIN
53.	mDL unterstützt das Übermittlungsprofil L2CAP, wenn es als GATT-Client für die Geräteabfrage über BLE fungiert.	☐ JA ☒ NEIN
54.	mdL unterstützt Geräteabfrage über BLE im Peripherieserver-Modus des Mdoc.	☒ JA ☐ NEIN
55.	mDL unterstützt das Übermittlungsprofil L2CAP, wenn es als GATT-Server für die Geräteabfrage über BLE fungiert.	☐ JA ☒ NEIN
56.	mDL unterstützt Geräteabfrage über Wi-Fi Aware.	☐ JA ☒ NEIN
57.	mDL unterstützt die Cipher Suite NCS-PK-2WDH-128 für Wi-Fi Aware.[5]	☐ JA ☒ NEIN
58.	mDL unterstützt Serverabfrage über OIDC	☐ JA ☒ NEIN
59.	mDL unterstützt Serverabfrage über WebAPI	☐ JA ☒ NEIN
60.	mDL unterstützt die Übermittlung von Serverabfrage-Informationen innerhalb der Geräteinteraktionsstruktur.	☐ JA ☒ NEIN
61.	mDL richtet für die Zeit zwischen dem Versand von Geräteinteraktionsdaten und dem Empfang der Mitteilung über den Aufbau der Sitzung ein Time-out ein, wenn die Geräteinteraktion über QR-Code erfolgt.	☐ JA ☒ NEIN
62.	Falls ja, geben Sie die Dauer des vom mDL eingerichteten Time-outs in Sekunden an.	Keine
63.	mDL richtet für die Zeit zwischen dem Versand von Geräteinteraktionsdaten und dem Empfang der Mitteilung über den Aufbau der Sitzung ein Time-out ein, wenn die Geräteinteraktion über NFC erfolgt.	☐ JA ☒ NEIN
64.	Falls ja, geben Sie die Dauer des vom mDL eingerichteten Time-outs in Sekunden an.	Keine

[4] Hinweis: NFC Static Handover und NFC Negotiated Handover können nicht gleichzeitig unterstützt werden, wenn ein mDL beide Technologien unterstützt.

[5] Gilt nur, wenn das Mdoc Wi-Fi Aware für die Geräteabfrage und NFC Negotiated Handover für die Geräteinteraktion unterstützt.

CONSORCIO EMDOC, S.R.L. EMDOC CONSORCIO Santo Domingo

fime.c

A.1.4 Für Sicherheitsmechanismus-Testfälle

710

Nr.	Erklärungen zur Konformität der Implementierung für Sicherheitsmechanismus-Testfälle	
65.	Welche Kurven unterstützt der mDL für den Aufbau von Sitzungen? Kreuzen Sie alle unterstützten Kurven an.[6]	☒ P-256 Kurve ☐ P-384 Kurve ☐ P-521 Kurve ☐ X25519 ☐ X448 ☐ brainpoolP256r1 ☐ brainpoolP320r1 ☐ brainpoolP384r1 ☐ brainpoolP512r1
66.	mDL unterstützt den Austausch von mehr als einer Mdoc-Anfrage und -Antwort zur Geräteabfrage mit dem Mdoc-Lesegerät in einer einzigen Sitzung.	☐ JA ☒ NEIN
67.	Falls ja, geben Sie die Dauer des vom mDL eingerichteten Time-outs für die Beendigung der Sitzung in Sekunden an.	
68.	Welche Kurven unterstützt die Behörde, die den mDL ausstellt, für die Authentifizierung von Ausstellerdaten? Kreuzen Sie alle unterstützten Kurven an.[7]	☒ P-256 Kurve ☐ P-384 Kurve ☐ P-521 Kurve ☐ Ed25519 ☐ Ed448 ☐ brainpoolP256r1 ☐ brainpoolP320r1 ☐ brainpoolP384r1 ☐ brainpoolP512r1
69.	mDL unterstützt Mdoc MAC-Authentifizierung.	☐ JA ☒ NEIN
70.	Falls ja, welche Kurven unterstützt der mDL für die Mdoc MAC-Authentifizierung? Kreuzen Sie alle unterstützten Kurven an.[8]	☐ P-256 Kurve ☐ P-384 Kurve ☐ P-521 Kurve ☐ X25519 ☐ X448 ☐ brainpoolP256r1

[6] Unterstützt der mDL mehrere Kurven für den Aufbau von Sitzungen, sollte der mDL-Eigentümer für Testzwecke jeweils ein Muster für jede unterstützte Kurve bereitstellen.

[7] Wenn auf dem mDL mehrere Dokumente vorhanden sind, kann die ausstellende Behörde theoretisch für die MSO-Unterzeichnung auf jedem dieser Dokumente eine andere Kurve verwenden. Es wird jedoch darauf hingewiesen, dass FIME davon ausgeht, dass für alle Dokumente auf einem Muster die gleiche Kurve verwendet wird. Für Testzwecke sollte der mDL-Eigentümer jeweils ein Muster für jede unterstützte Kurve bereitstellen.

[8] Wenn auf dem mDL mehrere Dokumente vorhanden sind, kann der mDL theoretisch für jedes dieser Dokumente eine andere Mdoc MAC-Authentifizierungskurve verwenden. Es wird jedoch darauf hingewiesen, dass FIME davon ausgeht, dass für alle Dokumente auf einem Muster die gleiche Kurve verwendet wird. Für Testzwecke sollte der mDL-Eigentümer jeweils ein Muster für jede unterstützte Kurve bereitstellen.

EMDOC CONSORCIO Santo Domingo, R.D.
fime.c

		☐ brainpoolP320r1 ☐ brainpoolP384r1 ☐ brainpoolP512r1
71.	mDL unterstützt Mdoc ECDSA-/EdDSA-Authentifizierung.	☒ JA ☐ NEIN
72.	Falls ja, welche Kurven verwendet der mDL für die Mdoc ECDSA-/EdDSA-Authentifizierung? Kreuzen Sie alle unterstützten Kurven an.[9]	☒ P-256 Kurve ☐ P-384 Kurve ☐ P-521 Kurve ☐ Ed25519 ☐ Ed448 ☐ brainpoolP256r1 ☐ brainpoolP320r1 ☐ brainpoolP384r1 ☐ brainpoolP512r1
73.	mDL unterstützt die Authentifizierung von Mdoc-Lesegeräten.	☒ JA ☐ NEIN
74.	Falls ja, welche Kurven unterstützt der mDL für die Authentifizierung von Mdoc-Lesegeräten? Kreuzen Sie alle unterstützten Kurven an.[10]	☒ P-256 Kurve ☒ P-384 Kurve ☒ P-521 Kurve ☐ Ed25519 ☐ Ed448 ☐ brainpoolP256r1 ☐ brainpoolP320r1 ☐ brainpoolP384r1 ☐ brainpoolP512r1
75.	Falls ja, benachrichtigt das Mdoc den Mdoc-Inhaber im Falle einer fehlgeschlagenen Authentifizierung des Mdoc-Lesegeräts darüber, dass die Identität des Prüfers nicht verifiziert werden konnte?	☒ JA ☐ NEIN
76.	Falls ja, gibt es Datenelemente, die das Mdoc im Falle einer fehlgeschlagenen Authentifizierung des Lesegeräts nicht freigibt? Bitte führen Sie diese ggf. anhand von Namensraum und Bezeichner auf.[11]	☐ JA, und zwar:... ☒ NEIN
77.	Falls ja, unterstützt Mdoc den Abruf von OCSP-Informationen, sofern vorhanden, zur Verifizierung eines Zertifikats für die	☐ JA ☒ NEIN

[9] Hinweis: Es können für jedes Dokument auf einem mDL mehrere SDeviceKey-Paare für die Mdoc-Authentifizierung, jeweils in einer eigenen MSO, vorhanden sein. Daher ist es theoretisch möglich, dass ein einzelnes Dokument abwechselnd MAC-Authentifizierung und ECDSA-/EdDSA-Authentifizierung oder abwechselnd unterschiedliche Kurven für die ECDSA-/EdDSA-Authentifizierung verwendet. Es wird jedoch darauf hingewiesen, dass FIME davon ausgeht, dass für alle Dokumente in einem Muster durchgängig die gleiche Mdoc-Authentifizierungsmethode (MAC oder ECDSA/EdDSA) verwendet wird. Außerdem geht FIME davon aus, dass für alle Dokumente in einem Muster die gleiche ECDSA-/EdDSA-Kurve verwendet wird. Für Testzwecke sollte der mDL-Eigentümer jeweils ein Muster für jede unterstützte Kurve bereitstellen.

[10] FIME geht davon aus, dass alle uns bereitgestellten mDL-Muster alle angekreuzten Kurven für die Authentifizierung von M[illegible] unterstützen (sofern die richtigen CA-Zertifikate installiert sind).

[11] Es sollte mindestens bei Nr. 75 ODER Nr. 76 JA angekreuzt werden. Andernfalls hat das Fehlschlagen der Authentifizierung eines Lesegeräts keinerlei Auswirkungen.

CONSORCIO EMDOC J.D. EMDOC CONSORCIO Santo Domingo
fime.c

	Authentifizierung von Mdoc-Lesegeräten?	
78.	Falls ja, unterstützt Mdoc den Abruf von CRL-Informationen zur Verifizierung eines Zertifikats für die Authentifizierung von Mdoc-Lesegeräten?	☒ JA ☐ NEIN
79.	Während der Tests steht eine vom Kunden bereitgestellte Test-CRL für alle IACA-Root-Zertifikate zur Verfügung.	☐ JA ☒ NEIN
80.	Während der Tests steht eine Test-CRL für alle vom Mdoc verwendeten Document Signer Zertifikate zur Verfügung.	☐ JA ☒ NEIN

A.1.5 Für Anwendungsfall-Testfälle

81.	Der mDL ermöglicht es dem mDL-Inhaber, seine Zustimmung zum Teilen des Lichtbilds zu verweigern, aber dennoch dem Teilen anderer im Rahmen derselben Anfrage angeforderter Datenelemente zuzustimmen.	☒ JA ☐ NEIN

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

713

Als Notar bestätige ich hiermit, dass dieses Dokument eine originalgetreue Abschrift des Originaldokuments ist.

München, den 29. Januar 2025

[Notarielles Siegel]

[Unterschrift]

Dr. Bernhard Schaub

Notar in München, Deutschland

(Kommission endet am 31. Oktober 2032)

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

Als vom Präsidenten des Landgerichts München I öffentlich bestellte und allgemein beeidigte Übersetzerin für die spanische und englische Sprache bestätige ich: Vorstehende Übersetzung des mir in englischer Sprache vorgelegten Dokuments ist richtig und vollständig.

München, den 06. Februar 2025

Unterschrift und Stempel: _____

Susanne Bernhardt – Ravensburger Ring 18 – 81243 München

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo

Certified Copy

715

Veridos
Oranienstraße 91, Berlin, Germany 10969
Berlin, Germany

2nd August 2024

Subject: Confirmation of conformity of Android-based Veridos Mobile ID Wallet Version 1.0.11 with ISO/IEC 18013-5:2021

Dear Mr. Nicholas,

This letter serves to confirm that the abovementioned mDL application ('the application') was tested by FIME and found to be compliant with ISO/IEC 18013-5:2021 as of the date of this letter.

The test scope included testing the application on its interface to an mDL reader, by executing the test cases listed in the latest draft version of ISO/IEC 18013-6. Testing was limited to the features supported by the application, as indicated in the Implementation Conformance Statement in the Appendix to this letter. Details of the application under test, the test environment, and the test devices used for testing can be found on the next page.

As a reminder, the correct functioning of the application is dependent on several factors in its operational environment. Veridos is solely and fully responsible for the conformity of the application to all applicable standards, specifications, and requirements.

The number of the Test Report corresponding to this letter is FIME_Veridos_Android_02. This report contains the full overview of executed test cases and all test results.

Yours sincerely,

FIME

David Bakker
Technical Lead

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

FIME Services North America Inc. 1945 The Exchange, Suite 200 SE, Atlanta, GA 30339, United States

714

mDL implementation scope

System Under Test

Application name and version	Veridos Mobile ID Wallet Version 1.0.11
Date of receipt of application	2024-07-23

Implementation Conformance Statement Summary

Device engagement technologies	QR code NFC Negotiated Handover
Device retrieval technologies	BLE in mdoc central client mode BLE in mdoc peripheral server mode
Server retrieval technologies	None
Security mechanisms for device retrieval	Session encryption, issuer data authentication, mdoc ECDSA/EdDSA authentication, mdoc reader authentication

Test Environment

Standard	ISO/IEC 18013-5:2021
Test Case Specification	FIME mDL Test Case Specification
Test tool	FIME mDL Application Test Suite v1.3.14
mDL test app	mdltestapp-1.3.1.apk
Test device on which the mDL test app is installed	Samsung Galaxy S20+ 5G
OS version of the test device on which the mDL test App is installed	Android 12

Test Devices and Platform

Device model and type	Samsung Galaxy S24
OS version	Android 14

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.
fimo.c

A.1 Implementation conformance statement

The Implementation Conformance Statements below were provided to FIME by Veridos and have been used to determine which test cases to execute.

The ICS version used by Veridos is v1.10.

A.1.1 General information

mDL owner	
Application owner Name	Veridos
Address	OranienstraBe 91
City	Berlin
State	Berlin
Zip Code / Postal Code	10969
Country	Germany
Contact Name	Nicholas Larter
Contact Title	Senior Solutions Manager
Contact Email Address	nick.larter@veridos.com
Contact Phone Number	+49 1525 1334198

#	mDL Application General Information	
•	Certification Type	☒ Functional [1] ☐ Integrated Product [2]
•	Application name and version	Veridos Mobile ID Wallet Version 1.0.11
•	Minimum version of Android supported	Android 10
	How many documents are present on the mDL under test?	1
	For each document, please specify the applicable DocType	org.iso.18013.5.1.mDL
	For each document, please specify all data element namespaces used by the document	org.iso.18013.5.1
	For each namespace different from the mDL namespace ("org.iso.18013.5.1"), please specify the identifiers of all data elements present in the document	

[1] For functional certification, the mDL data set can be a sample data set that the mDL owner would like to personalize onto the mDL.
[2] Integrated product certification requires the mDL data set to be prepared and personalized by an Issuer System in Record (SoR) and the mDL data set shall be a representative of the mDL that will be used in production.
3

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

718

A.1.2 For mdl data model test cases

Note: all the data elements in this section are in the default mDL data namespace ("org.iso.18013.5.1"). The ICS statements in this section have to be filled in only for documents having DocType = "org.iso.18013.5.1.mDL".

#	ICS statements for mDL Data Model test cases[3]	
5.	Data element administrative_number is present in the mDL data.	☐YES ☒NO
6.	Data element sex is present in the mDL data.	☒YES ☐NO
7.	Data element height is present in the mDL data.	☒YES ☐NO
8.	Data element weight is present in the mDL data.	☐YES ☒NO
9.	Data element eye_color is present in the mDL data.	☒YES ☐NO
10.	Data element hair_color is present in the mDL data.	☒YES ☐NO
11.	Data element birth_place is present in the mDL data.	☒YES ☐NO
12.	Data element resident_address is present in the mDL data.	☒YES ☐NO
13.	Data element portrait_capture_date is present in the mDL data.	☒YES ☐NO
14.	Data element age_in_years is present in the mDL data.	☒YES ☐NO
15.	Data element age_birth_year is present in the mDL data.	☒YES ☐NO
16.	Data element age_over_NN is present in the mDL data. In case you select YES, please provide six (6) age_over_NN data elements in the mDL data, of which three (3) lower NN values with the value TRUE and three (3) higher values with the value FALSE. Please make sure the set of age_over_NN data elements is consistent. List the values for NN1 – NN6 present in the mDL data.	☐YES ☒NO

[3] Note: all data elements in this section are in the default mDL data namespace ("org.iso.18013.5.1"). The ICS statements in this section should be filled in only for documents having DocType = "org.iso.18013.5.1.mDL".

CONSORCIO EMDOC Santo Domingo

fime.c

Value for NN in data element identifier	Value (TRUE / FALSE)
age_over_NN1(L)	TRUE
age_over_NN2(L)	TRUE
age_over_NN3(L)	TRUE
age_over_NN4(H)	FALSE
age_over_NN5(H)	FALSE
age_over_NN6(H)	FALSE

EXAMPLE: The following set complies with the above rules:

age_over_15 = TRUE (NN1 = 15)
age_over_18 = TRUE (NN2 = 18)
age_over_21 = TRUE (NN3 = 21)
age_over_60 = FALSE (NN4 = 60)
age_over_65 = FALSE (NN5 = 65)
age_over_68 = FALSE (NN6 = 68)

17.	Data element issuing_jurisdiction is present in the mDL data.	☐YES ☒NO
18.	Data element nationality is present in the mDL data.	☒YES ☐NO
19.	Data element resident_city is present in the mDL data.	☒YES ☐NO
20.	Data element resident_state is present in the mDL data.	☒YES ☐NO
21.	Data element resident_postal_code is present in the mDL data.	☒YES ☐NO
22.	Data element resident_country is present in the mDL data.	☒YES ☐NO
23.	Data element biometric_template_face is present in the mDL data.	☐YES ☒NO
24.	Data element biometric_template_voice is present in the mDL data.	☐YES ☒NO
25.	Data element biometric_template_finger is present in the mDL data.	☐YES ☒NO
26.	Data element biometric_template_iris is present in the mDL data.	☐YES ☒NO
27.	Data element biometric_template_retina is present in the mDL data.	☐YES ☒NO
28.	Data element biometric_template_hand_geometry is present in the mDL data.	☐YES ☒NO

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

29.	Data element biometric_template_signature_sign is present in the mDL data.	☐YES ☒NO
30.	Data element biometric_template_keystroke is present in the mDL data.	☐YES ☒NO
31.	Data element biometric_template_lip_movement is present in the mDL data.	☐YES ☒NO
32.	Data element biometric_template_thermal_face is present in the mDL data.	☐YES ☒NO
33.	Data element biometric_template_thermal_hand is present in the mDL data.	☐YES ☒NO
34.	Data element biometric_template_gait is present in the mDL data.	☐YES ☒NO
35.	Data element biometric_template_body_odor is present in the mDL data.	☐YES ☒NO
36.	Data element biometric_template_dna is present in the mDL data.	☐YES ☒NO
37.	Data element biometric_template_ear is present in the mDL data.	☐YES ☒NO
38.	Data element biometric_template_finger_geometry is present in the mDL data.	☐YES ☒NO
39.	Data element biometric_template_palm_geometry is present in the mDL data.	☐YES ☒NO
40.	Data element biometric_template_vein_pattern is present in the mDL data.	☐YES ☒NO
41.	Data element biometric_template_foot_print is present in the mDL data.	☐YES ☒NO
42.	Data element family_name_national_character is present in the mDL data.	☐YES ☒NO
43.	Data element given_name_national_character is present in the mDL data.	☐YES ☒NO
44.	Data element signature_usual_mark is present in the mDL data.	☐YES ☒NO

A.1.3 For technology test cases

#	ICS statements for Technology test cases	
45.	mDL supports device engagement using NFC Static Handover.	☐YES ☒NO

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R D

46.	mDL supports device engagement using NFC Negotiated Handover.[4]	☒YES ☐NO
47.	mDL supports device engagement using QR code.	☒YES ☐NO
48.	mDL supports device retrieval using NFC.	☐YES ☒NO
49.	mDL supports extended-length APDUs for device retrieval using NFC.	☐YES ☒NO
50.	mDL supports BLE version 4.2 (or above) and LE Data Packet Length Extension.	☒YES ☐NO
51.	mDL supports device retrieval using BLE in mdoc central client mode.	☒YES ☐NO
52.	If BLE in mdoc central client mode is used for device retrieval, mdoc verifies the value of the Ident characteristic.	☐YES ☒NO
53.	mDL supports the L2CAP transmission profile if it is acting as the GATT client for device retrieval using BLE.	☐YES ☒NO
54.	mDL supports device retrieval using BLE in mdoc peripheral server mode.	☒YES ☐NO
55.	mDL supports the L2CAP transmission profile if it is acting as the GATT server for device retrieval using BLE.	☐YES ☒NO
56.	mDL supports device retrieval using Wi-Fi Aware.	☐YES ☒NO
57.	mDL supports the NCS-PK-2WDH-128 cipher suite for Wi-Fi Aware.[5]	☐YES ☒NO
58.	mDL supports server retrieval using OIDC	☐YES ☒NO
59.	mDL supports server retrieval using WebAPI	☐YES ☒NO
60.	mDL supports transferring server retrieval information in the device engagement structure	☐YES ☒NO
61.	mDL implements a time-out for the time between sending device engagement data and receiving the session establishment message when using QR code for device engagement.	☐YES ☒NO
62.	If yes, how many seconds is the time-out period implemented by the mDL?	None
63.	mDL implements a time-out for the time between sending device engagement data and receiving the session establishment message when using NFC for device engagement.	☐YES ☒NO

[4] Note that NFC Static Handover and NFC Negotiated Handover cannot be supported simultaneously if an mDL supports both technologies

[5] Only applicable in case the mdoc supports Wi-Fi Aware for device retrieval and supports NFC Negotiated Handover for device engagement.

7

CONSORCIO EMDOC, EMDOC, CONSORCIO, Santo Domingo, R.D.

fime.c

64.	If yes, how many seconds is the time-out period implemented by the mDL?	None

A.1.4 For security mechanism test cases

#	ICS statements for Security Mechanisms test case	
65.	Which curves does the mDL support for session establishment? Select all that are supported.[6]	☒ Curve P-256 ☐ Curve P-384 ☐ Curve P-521 ☐ X25519 ☐ X448 ☐ brainpoolP256r1 ☐ brainpoolP320r1 ☐ brainpoolP384r1 ☐ brainpoolP512r1
66.	mDL supports exchanging more than one device retrieval mdoc request and response with the mdoc reader in a single session.	☐YES ☒NO
67.	If yes, how many seconds is the time-out period for session termination implemented by the mDL?	
68.	Which curves does the mDL issuing authority support for issuer data authentication? Select all that are supported.[7]	☒ Curve P-256 ☐ Curve P-384 ☐ Curve P-521 ☐ Ed25519 ☐ Ed448 ☐ brainpoolP256r1 ☐ brainpoolP320r1 ☐ brainpoolP384r1 ☐ brainpoolP512r1
69.	The mDL supports mdoc MAC authentication.	☐YES ☒NO
70.	If yes, which curves does the mDL support for mdoc MAC authentication? Select all that are supported.[8]	☐ Curve P-256 ☐ Curve P-384 ☐ Curve P-521 ☐ X25519

6 If the mDL supports multiple curves for session establishment, then for the purpose of testing, the mDL owner should provide a separate sample for each of the curves supported.
7 If multiple documents are present on the mDL, the issuing authority can in theory use a different curve for signing the MSO on each of them. However, please note that FIME expects that the same curve is used for all documents on a given sample. For the purpose of testing, the mDL owner should provide a separate sample for each of the curves supported.
8 If multiple documents are present on the mDL, the mDL can in theory use a different mdoc MAC authentication curve for each of them. However, please note that FIME expects that the same curve is used for all documents on a given sample. For the purpose of testing, the mDL owner should provide a separate sample for each of the curves supported.
a

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R D

		☐ X448 ☐ brainpoolP256r1 ☐ brainpoolP320r1 ☐ brainpoolP384r1 ☐ brainpoolP512r1
71.	The mDL supports mdoc ECDSA/EdDSA authentication	☒ YES ☐ NO
72.	If yes, which curves does the mDL use for mdoc ECDSA/EdDSA authentication? Select all that are supported.[9]	☒ Curve P-256 ☐ Curve P-384 ☐ Curve P-521 ☐ Ed25519 ☐ Ed448 ☐ brainpoolP256r1 ☐ brainpoolP320r1 ☐ brainpoolP384r1 ☐ brainpoolP512r1
73.	The mDL supports mdoc reader authentication	☒ YES ☐ NO
74.	If yes, which curves does the mdoc support for mdoc reader authentication? Select all that are supported.[10]	☒ Curve P-256 ☒ Curve P-384 ☒ Curve P-521 ☐ Ed25519 ☐ Ed448 ☐ brainpoolP256r1 ☐ brainpoolP320r1 ☐ brainpoolP384r1 ☐ brainpoolP512r1
75.	If yes, if mdoc reader authentication fails, does the mdoc notify the mdoc holder that the mdoc verifier's identity could not be verified?	☒ YES ☐ NO
76.	If yes, are there any data elements that the mdoc will not release if reader authentication fails? If so, please list them all by namespace and identifier. [11]	☐ YES, namely... ☒ NO

9 Note that for each document on an mDL, there could potentially be multiple SDeviceKey pairs for mdoc authentication, each in a separate MSO. It is therefore theoretically possible that a single document uses MAC authentication and ECDSA/EdDSA authentication alternatingly or uses different curves for ECDSA/EdDSA alternatingly. However, please note that FIME expects that the same mdoc authentication mechanism (either MAC or ECDSA/EdDSA) is consistently used for all documents on a given sample. Moreover, FIME expects that the same ECDSA/EdDSA curve is used for all documents on a given sample. For testing, the mDL owner should provide a separate sample for each of the curves supported.

10 FIME assumes that all mDL samples provided to us will support all mdoc reader authentication curves selected (provided that the correct CA certificates are installed).

11 At least one of ICS #75 and ICS #76 should be answered with Yes. Otherwise, failing reader authentication would not have any consequences.

CONSORCIO EMDOC, EMDOC CONSORCIO, Santo Domingo, R. D.

77.	If yes, mdoc supports retrieving OCSP information, if available, when verifying an mdoc reader authentication certificate.	☐YES ☒NO
78.	If yes, mdoc supports retrieving CRL information when verifying a mdoc reader authentication certificate	☒YES ☐NO
79.	A test CRL for all IACA root certificates provided by the customer is available during testing.	☐YES ☒NO
80.	A test CRL for all Document Signer certificates used by the mdoc is available during testing.	☐YES ☒NO

A.1.5 For use case test cases

#	ICS statements for Use Cases test cases	
81.	The mDL enables the mDL holder to refuse consent for sharing the portrait but give consent for sharing other data elements requested in the same request.	☒YES ☐NO

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R D

725

I, Notary Public, hereby certify that this document is a true copy of the original document.

Munich, this 29.01.2025

Dr. Bernhard Schaub
Notary Public in Munich,
Federal Republic of Germany
(commission expires: October 31, 2032)

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

726

Öffentlich bestellte und beeidigte Übersetzerin für die spanische Sprache
Susanne Bernhardt
Rosenstorgar Ring 18
81243 München

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

727

Traducción jurada del alemán

Traducción jurada del inglés

[Logotipo de la empresa firma] Copia notarial

Veridos
Nicholas Larter
Oranienstraße 91, 10969 Berlín

27 de agosto de 2024

Asunto: Confirmación de la conformidad del VD CheckID basado en Android, versión 1.0.12 (12) con la norma ISO/IEC 18013-5:2021

Estimado Sr. Larter:

Nos dirigimos a usted para confirmarle que el lector mDL mencionado anteriormente ha sido probado por FIME y ha resultado ser conforme con la norma ISO/IEC 18013-5:2021 a partir de la fecha de esta carta.

Parte de las pruebas consistió en comprobar la interfaz del lector mDL con un mDL mediante la ejecución de los casos de prueba enumerados en la última versión del borrador de la norma ISO/IEC 18013-6. Solo se realizaron aquellas pruebas compatibles con las funciones del lector mDL, tal y como se especifica en la Declaración de Conformidad de la implementación adjunta a esta carta. Para más información sobre la aplicación probada, el entorno de prueba y el equipo utilizado para la prueba, consulte la página siguiente.

Debe tenerse en cuenta que el correcto funcionamiento del lector mDL depende de diversos factores dentro de su entorno operativo. Veridos es el único y pleno responsable de la conformidad del lector mDL con todas las normas, especificaciones y requisitos aplicables.

El informe de pruebas que acompaña a esta carta lleva el número FIME_eID_Veridos_Android_01. Este protocolo contiene una descripción completa de los casos de prueba ejecutados y todos los resultados de las pruebas.

Atentamente
[Firma]

FIME

David Bakker
Director técnico

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

728

Ámbito de aplicación de mDL

Sistema probado

Nombre y versión de la aplicación	VD CheckID Versión 1.0.12(12)
Aplicación recibida el	23 de julio de 2024

Resumen de la declaración de conformidad de la aplicación

Tecnologías para la interacción con el dispositivo	Código QR NFC Static Handover NFC Negotiated Handover
Tecnologías para la consulta de dispositivos	BLE en el modo cliente central del Mdoc BLE en el modo servidor periférico del Mdoc NFC
Tecnologías para la consulta del servidor	Ninguna
Mecanismos de seguridad para la consulta del dispositivo	Cifrado de las sesiones, autentificación de los datos del emisor, autentificación Mdoc ECDSA/EdDSA, autentificación de los lectores Mdoc

Entorno de prueba

Norma	ISO/IEC 18013-5: 2021
Especificación de casos de prueba	Especificación de casos de prueba FIME para el lector mDL
Conjunto de pruebas	FIME Test Suite v1.4.0 para el lector mDL
Aplicación de prueba mDL	mdlreadertestapp-1.4.0.apk
Dispositivo de prueba en el que está instalada la aplicación de prueba mDL	Samsung Galaxy S20+ 5G
Versión del sistema operativo del dispositivo de prueba en el que está instalada la aplicación de prueba mDL	Android 12

Dispositivos de prueba y plataforma

Marca y tipo de dispositivo	Samsung Galaxy S24	Google Pixel 3a
Versión del sistema operativo	Android 14	Android 12

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

fime.com

729

A.1 Declaración de conformidad de la implementación

Veridos envió a la FIME las siguientes declaraciones de conformidad de la implementación (Implementation Conformance Statement, ICS). Se han utilizado para determinar los casos de prueba que deben ejecutarse.

Veridos utiliza la versión v1.6 de ICS.

A.1.1 Información general

Propietario del mDL	
Nombre del propietario de la aplicación	Veridos
Dirección	Oranienstraße 91, 10969 Berlin
Ciudad	Berlin
Estado Federal	Berlin
C.P.	10969
País	Alemania
Nombre de la persona de contacto	Nicholas Larter
Cargo	Senior Solutions Manager
Correo electrónico de la persona de contacto	nick.larter@veridos.com
Número de teléfono de la persona de contacto	+49 1525 1334198

N.º	Información general sobre el lector mDL	
-	Nombre y versión de la aplicación del lector	VD CheckID Versión 1.0.12(12)
-	Versión de Android compatible más baja	Android 12

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.
fime.com

1.	Especifique qué DocType(s) admite el lector mDL	1
2.	Para cada DocType, especifique qué espacio(s) de nombres admite el lector mDL.	org.iso.18013.5.1.mDl
3.	Para cada espacio de nombres, introduzca los identificadores de todos los elementos de datos que pueden ser consultados por el lector mDL.	family_name given_name birth_date document_number driving_privileges issue_date expiry_date issuing_authority issuing_country portrait un_distinguishing_sign sex height weight eye_colour hair_colour age_in_years age_birth_year birth_place nationality portrait_capture_date resident_address resident_city resident_state resident_postal_code resident_country signature_usual_mark family_name_national_character given_name_national_character age_over_18 age_over_19 age_over_20 age_over_21 age_over_22 age_over_23 age_over_24 age_over_25 age_over_26
4.	El lector mDL es capaz de solicitar múltiples documentos en un único mensaje DeviceRequest. [1]	☐ SÍ ☒ NO
5.	El lector mDL es capaz de solicitar múltiples documentos en un único mensaje DeviceRequest. [2] [3]	☐ SÍ ☒ NO

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

time.com

6.	El lector mDL puede consultar el elemento de datos «issuing_jurisdiction» del espacio de nombres «org.iso.18013.5.1».	☐ SÍ ☒ NO
7.	El lector mDL puede consultar el elemento de datos «age_over_NN» del espacio de nombres «org.iso.18013.5.1».	☒ SÍ ☐ NO
8.	El lector mDL puede consultar el elemento de datos «issuing_country» del espacio de nombres «org.iso.18013.5.1».	☒ SÍ ☐ NO

A.1.2 Para casos de pruebas de tecnología

N.º	Declaraciones de conformidad de la implementación para los casos de prueba de tecnología	
9.	El lector Mdoc admite la interacción de dispositivos mediante el traspaso estático NFC. [4]	☒ SÍ ☐ NO
10.	El lector Mdoc es compatible con la interacción de dispositivos vía NFC Negotiated Handover. [5]	☒ SÍ ☐ NO
11.	El lector Mdoc admite la interacción de dispositivos mediante un código QR. [4]	☒ SÍ ☐ NO
12.	El lector Mdoc admite consultas de dispositivos mediante NFC. [4]	☒ SÍ ☐ NO
13.	El lector Mdoc admite consultas de dispositivos a través de BLE en el modo de cliente central del Mdoc. [1]	☒ SÍ ☐ NO
14.	El lector Mdoc admite consultas de dispositivos a través de BLE en el modo de servidor periférico del Mdoc. [4]	☒ SÍ ☐ NO
15.	El lector Mdoc admite la consulta de dispositivos mediante BLE versión 5.0 (o superior) y LE 2M PHY.	☐ SÍ ☒ NO
16.	El lector Mdoc admite consultas de dispositivos a través de Wi-Fi Aware.	☐ SÍ ☒ NO
17.	El lector Mdoc admite consultas al servidor a través de OIDC	☐ SÍ ☒ NO
18.	El lector Mdoc admite consultas al servidor a través de WebAPI.	☐ SÍ ☒ NO
19.	El lector Mdoc admite APDUs extralargos para consultas de dispositivos a través de NFC.	☒ SÍ ☐ NO
20.	El lector Mdoc admite el perfil de transmisión L2CAP cuando actúa como cliente GATT para la consulta de dispositivos a través de BLE.	☐ SÍ ☒ NO
21.	El lector Mdoc admite el perfil de transmisión L2CAP si actúa como servidor GATT para la consulta de dispositivos a través de BLE.	☐ SÍ ☒ NO
22.	El lector Mdoc envía una estructura ReaderEngagement como parte del mensaje Handover Request Message durante la interacción con el dispositivo a través de un NFC Negotiated	☒ NO



	Handover.	
23.	El lector Mdoc establece un Time-out para el periodo entre la inicialización de la transacción y la recepción de los datos de interacción del dispositivo.	☐ SÍ ☒NO
24.	Si selecciona SÍ, introduzca la duración del Time-out (en segundos).	xx segundos
25.	El lector Mdoc establece un Time-out para el periodo entre la recepción de los datos de interacción del dispositivo y el establecimiento satisfactorio de una conexión de consulta del dispositivo.	☐ SÍ ☒NO
26.	Si selecciona SÍ, introduzca la duración del Time-out (en segundos).	xx segundos

A.1.3 Para casos de prueba de mecanismos de seguridad

Nº	Declaraciones de conformidad de la implementación para los casos de prueba de mecanismos de seguridad	
27.	El lector Mdoc es compatible con la autenticación de lectores Mdoc.	☒SÍ ☐ NO
28.	Si se selecciona SÍ, durante la comprobación se dispone de una CRL de prueba para todos los certificados de autenticación de lectores Mdoc utilizados por el lector Mdoc.	☒SÍ ☐ NO
29.	Si se selecciona SÍ, la autoridad de certificación que ha firmado todos los certificados de autenticación de lectores Mdoc utilizados por el lector Mdoc dispone de un servicio OCSP.	☐ SÍ ☒NO
30.	Si se selecciona SÍ, se dispone de un OCSP-Responder de prueba durante la comprobación de todos los certificados de autenticación para lectores Mdoc utilizados por el lector Mdoc.	☐ SÍ ☒NO
31.	Si se selecciona SÍ, ¿qué curva utiliza el lector Mdoc para la autenticación de los lectores Mdoc? Seleccione una respuesta.	☒ Curva P-256 ☒ Curva P-384 ☒ Curva P-521 ☒ Ed25519 ☒ Ed448 ☒ brainpoolP256r1 ☒ brainpoolP320r1 ☒ brainpoolP384r1 ☒ brainpoolP512r1
32.	El lector de Mdoc admite el intercambio de más de una solicitud y respuesta de Mdoc para la consulta del dispositivo en el Mdoc en una única sesión.	☐ SÍ ☒NO
33.	El lector Mdoc admite el intercambio de más de una solicitud y respuesta para la consulta del servidor en la Infraestructura de la autoridad de certificación emisora en una única sesión.	☐ SÍ ☒NO
34.	El lector Mdoc admite la recuperación de información OCSP (si está disponible) al verificar un certificado de servidor TLS. [5]	☐ SÍ ☒NO

CONSORCIO EMDOC
EMDOC CONSORCIO
Santo Domingo, R.D.

35.	El lector Mdoc consulta la información de estado OCSP del certificado del servidor en el protocolo de enlace TLS. [1]	☐ SÍ ☒ NO
36.	El lector Mdoc admite TLS v 1.3. [3]	☐ SÍ ☒ NO
37.	El lector Mdoc admite la autenticación de clientes TLS.	☐ SÍ ☒ NO
38.	Si se selecciona SÍ, se dispone de una CRL de prueba durante la comprobación para todos los certificados de cliente TLS utilizados por el lector Mdoc	☐ SÍ ☒ NO
39.	Si se selecciona SÍ en el punto 34, la autoridad de certificación que ha firmado todos los certificados de autenticación de clientes TLS utilizados por el lector Mdoc dispone de un servicio OCSP.	☐ SÍ ☒ NO
40.	Si se selecciona SÍ, se dispone de un OCSP-Responder de prueba durante la comprobación de todos los certificados de autenticación de cliente TLS utilizados por el lector Mdoc.	☐ SÍ ☒ NO
41.	¿Cuántos segundos dura el Time-out de finalización de sesión establecido por el lector Mdoc?	300 segundos

[1] Si se selecciona SÍ, el lector mDL debe de apoyar por lo menos dos diferentes DocTypes.
[2] Esa declaración sólo es aplicable si el lector mDL apoya consultas al servidor a través de WebAPI.
[3] Si se selecciona SÍ, el lector mDL debe de apoyar por lo menos dos dos diferentes DocTypes.
[4] Por favor tenga en cuenta que eso es mandatorio para apoyar lectores mDL, pero opcional para lectores mdoc en general.
[5] Esa declaración sólo es aplicable si el lector mdoc apoya consultas al servidor a través de WebAPI.



fime.com

Yo, representante notarial, certifico que este documento es una copia fiel de un archivo pdf.

En Múnich, a 15/01/2025

[Sello del notario]

[Firma]

Dr. Christian Linke,

representante notarial de

Dr. Bernhard Schaub
Notario en Múnich,
República Federal de Alemania
(el mandato expira el 31 de octubre de 2032)

Por la presente se certifica la autenticidad de la firma precedente del Dr. Christian Linke, representante notarial, y del sello aquí estampado.
Asimismo, se certifica que la persona arriba mencionada estaba autorizada para llevar a cabo este acto oficial.

Múnich, 16 de enero de 2025
El Presidente del Tribunal Regional I de Múnich [Landgericht]
Por poder

[Firma ilegible]

Lea Adelsberger
Empleada del Tribunal

[Sello redondo del Tribunal Regional de Múnich, Baviera]

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo

Als in Bayern öffentlich bestellte und allgemein beeidigte Dolmetscherin für die englische und spanische Sprache bestätige ich: Vorstehende Übersetzung des mir in englischer Sprache als beglaubigte Abschrift vorgelegten Dokuments ist richtig und vollständig.

München, den 01. Februar 2025

Como traductora jurada y nombrada públicamente para los idiomas alemán, inglés y español en Baviera, confirmo que la traducción que precede de la copia certificada del documento que se me ha presentado en lengua inglesa es correcta y completa.

Múnich, a 1 de febrero del 2025

Unterschrift und Stempel:

Firma y sello:

Susanne Bernhardt – Ravensburger Ring 18 – 81243 München

Die Echtheit vorstehender Unterschrift der Übersetzerin Susanne Bernhardt wird hiermit bestätigt. Zugleich wird bescheinigt, dass die Vorgenannte öffentlich bestellte und allgemein beeidigte Übersetzerin für die spanische Sprache ist.

München, 07. Februar 2025
Die Präsidentin des Landgerichts München I
Im Auftrag

Justizsekretärin

736



ROCIO PELLERANO
MINISTRA CONSEJERA

EMBAJADA DE LA REPÚBLICA DOMINICANA
EN ALEMANIA
SECCIÓN CONSULAR

CERTIFICO, que la firma **que aparece** en la de esta documentación **es la** de la Sr./a. LEA- JUSTICIA REGIONAL
CIUDAD MUNCHEN **es la misma que acostumbra a us.** en sus **actos y la cual es de su entero crédito.**
FECHA 12.02.2025

95L

737

Beglaubigte Übersetzung aus dem Englischen

[Firmenlogo von fime] Beglaubigte Abschrift

Veridos
Nicholas Larter
Oranienstraße 91, 10969 Berlin

27. August 2024

Betreff: Bestätigung der Konformität der auf Android basierenden VD CheckID, Version 1.0.12 (12) mit ISO/IEC 18013-5:2021

Sehr geehrter Herr Larter,

mit diesem Schreiben bestätigen wir, dass das oben genannte mDL-Lesegerät von FIME getestet und im Ergebnis festgestellt wurde, dass es mit Stand zum Datum dieses Schreibens der Norm ISO/IEC 18013-5:2021 entspricht.

Teil des Testumfangs war die Prüfung des mDL-Lesegeräts auf seiner Schnittstelle zu einem mDL durch Ausführung der in der neuesten Entwurfsfassung von ISO/IEC 18013-6 aufgeführten Testfälle. Die Prüfung bezog sich nur auf vom mDL-Lesegerät unterstützte Funktionen, wie in der diesem Schreiben beigefügten Erklärung zur Konformität der Implementierung angegeben. Nähere Informationen zu der getesteten Anwendung, der Testumgebung und den für den Test verwendeten Prüfgeräten sind der folgenden Seite zu entnehmen.

Es wird darauf hingewiesen, dass die ordnungsgemäße Funktion des mDL-Lesegeräts von verschiedenen Faktoren innerhalb ihrer Betriebsumgebung abhängt. Für die Konformität des mDL-Lesegeräts mit allen geltenden Normen, Spezifikationen und Anforderungen trägt Veridos die alleinige und volle Verantwortung.

Das zu diesem Schreiben gehörende Prüfprotokoll trägt die Nummer FIME_eID_Veridos_Android_01. Dieses Protokoll enthält eine vollständige Übersicht der ausgeführten Testfälle und aller Testergebnisse.

Mit freundlichen Grüßen
[Unterschrift]

FIME

David Bakker
Technischer Leiter

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

FIME Services North America Inc, 1945 The Exchange, Suite 200 SE, Atlanta, GA 30339, United States

mDL-Implementierungsumfang

Getestetes System

Bezeichnung und Version der Anwendung	VD CheckID Version 1.0.12(12)
Anwendung erhältlich am	23. Juli 2024

Zusammenfassung der Erklärung zur Konformität der Implementierung

Technologien zur Datenextraktion	QR-Code NFC Static Handover NFC Negotiated Handover
Technologien zur Geräteabfrage	BLE im zentralen Client-Modus des Mdoc BLE im Peripherieserver-Modus des Mdoc NFC
Technologien zur Serverabfrage	Keine
Sicherheitsmechanismen für die Geräteabfrage	Verschlüsselung von Sitzungen, Authentifizierung von Ausstellerdaten, Mdoc ECDSA-/EdDSA-Authentifizierung, Authentifizierung von Mdoc-Lesegeräten

Testumgebung

Standard	ISO/IEC 18013-5: 2021
Testfallspezifikation	FIME Testfallspezifikation für mDL-Lesegerät
Test Suite	FIME Test Suite v1.4.0 für mDL-Lesegerät
mDL Testapp	mdlreadertestapp-1.4.0.apk
Prüfgerät, auf dem die mDL Testapp installiert ist	Samsung Galaxy S20+ 5G
Version des Betriebssystems auf dem Prüfgerät, auf dem die mDL Testapp installiert ist	Android 12

Prüfgeräte und -plattform

Marke und Typ des Geräts	Samsung Galaxy S24	Google Pixel 3a
Version des Betriebssystems	Android 14	Android 12

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

fime.com

A.1 Erklärung zur Konformität der Implementierung

Die folgenden Erklärungen zur Konformität der Implementierung (Implementation Conformance Statement, ICS) wurden FIME von Veridos vorgelegt. Anhand dieser wurde ermittelt, welche Testfälle auszuführen sind.

Veridos verwendet die ICS-Version v1.6.

A.1.1 Allgemeine Informationen

mDL-Eigentümer	
Name des Eigentümers der Anwendung	Veridos
Anschrift	Cranienstraße 91, 10969 Berlin
Stadt	Berlin
Bundesland	Berlin
PLZ	10969
Land	Deutschland
Name des Ansprechpartners	Nicholas Larter
Positionsbezeichnung	Senior Solutions Manager
E-Mail-Adresse des Ansprechpartners	nick.larter@veridos.com
Telefonnummer des Ansprechpartners	+49 1525 1334198

Nr.	Allgemeine Informationen zum mDL-Lesegerät	
-	Bezeichnung und Version der Lesegeräteanwendung	VD CheckID Version 1.0.12(12)
-	Niedrigste unterstützte Android-Version	Android 12



740

1.	Geben Sie an, welche DocType(s) vom mDL-Lesegerät unterstützt werden	1
2.	Geben Sie für jeden DocType an, welche Namespace(s) vom mDL-Lesegerät unterstützt werden.	org.iso.18013.5.1.mdl
3.	Geben Sie für jeden Namespace die Kennungen aller Datenelemente an, die vom mDL-Lesegerät abgefragt werden können.	family_name given_name birth_date document_number driving_privileges issue_date expiry_date issuing_authority issuing_country portrait un_distinguishing_sign sex height weight eye_colour hair_colour age_in_years age_birth_year birth_place nationality portrait_capture_dat e resident_address resident_city resident_state resident_postal_code resident_country signature_usual_mark family_name_national_character given_name_national_character age_over_18 age_over_19 age_over_20 age_over_21 age_over_22 age_over_23 age_over_24 age_over_25 age_over_26
4.	Das mDL-Lesegerät ist in der Lage, mehrere Dokumente in einer einzigen DeviceRequest-Meldung abzufragen. [1]	☐ JA ☒ NEIN

CONSORCIO EMDOC
EMDOC CONSORCIO
Santo Domingo, R D

fime.com

5.	Das mDL-Lesegerät ist in der Lage, mehrere Dokumente in einer einzigen ServerRequest-Meldung abzufragen. [2] [3]	☐ JA ☒ NEIN
6.	Das mDL-Lesegerät ist in der Lage, das „issuing_jurisdiction"-Datenelement vom Namespace „org.iso.18013.5.1" abzufragen	☐ JA ☒ NEIN
7.	Das mDL-Lesegerät ist in der Lage, das „age_over_NN"-Datenelement vom Namespace „org.iso.18013.5.1" abzufragen	☒ JA ☐ NEIN
8.	Das mDL-Lesegerät ist in der Lage, das „issuing_country"-Datenelement vom Namespace „org.iso.18013.5.1" abzufragen	☒ JA ☐ NEIN

A.1.2 Für Technologie-Testfälle

Nr.	Erklärungen zur Konformität der Implementierung für Technologie-Testfälle	
9.	Das Mdoc-Lesegerät unterstützt Geräteinteraktion über NFC Static Handover. [4]	☒ JA ☐ NEIN
10.	Das Mdoc-Lesegerät unterstützt Geräteinteraktion über NFC Negotiated Handover. [4]	☒ JA ☐ NEIN
11.	Das Mdoc-Lesegerät unterstützt Geräteinteraktion über einen QR-Code. [4]	☒ JA ☐ NEIN
12.	Das Mdoc-Lesegerät unterstützt Geräteabfrage über NFC. [4]	☒ JA ☐ NEIN
13.	Das Mdoc-Lesegerät unterstützt Geräteabfrage über BLE im zentralen Client-Modus des Mdoc. [4]	☒ JA ☐ NEIN
14.	Das Mdoc-Lesegerät unterstützt Geräteabfrage über BLE im Peripherieserver-Modus des Mdoc. [4]	☒ JA ☐ NEIN
15.	Das Mdoc-Lesegerät unterstützt Geräteabfrage über BLE Version 5.0 (oder höher) und LE 2M PHY.	☐ JA ☒ NEIN
16.	Das Mdoc-Lesegerät unterstützt Geräteabfrage über Wi-Fi Aware.	☐ JA ☒ NEIN
17.	Das Mdoc-Lesegerät unterstützt Serverabfrage über OIDC	☐ JA ☒ NEIN
18.	Das Mdoc-Lesegerät unterstützt Serverabfrage über WebAPI.	☐ JA ☒ NEIN
19.	Das Mdoc-Lesegerät unterstützt überlange APDUs für die Geräteabfrage über NFC.	☒ JA ☐ NEIN

[1] Falls hier JA ausgewählt wird, sollte das mDL-Lesegerät mindestens zwei verschiedene DocTypes unterstützen.
[2] Diese Aussage trifft nur zu, falls das mDL-Lesegerät Serverabfragen über WebAPI unterstützt.
[3] Falls hier JA ausgewählt wird, sollte das mDL-Lesegerät mindestens zwei verschiedene DocTypes unterstützen.
[4] Dies ist zur Unterstützung von mDL Lesegeräten obligatorisch, jedoch optional für Mdoc-Lesegeräte im Allgemeinen.

CONSORCIO EMDOC, EMDOC, CONSORCIO, Santo Domingo, R D
fime.com

20.	Das Mdoc-Lesegerät unterstützt das Übermittlungsprofil L2CAP, wenn es als GATT-Client für die Geräteabfrage über BLE fungiert.	☐ JA ☒ NEIN
21.	Das Mdoc-Lesegerät unterstützt das Übermittlungsprofil L2CAP, wenn es als GATT-Server für die Geräteabfrage über BLE fungiert.	☐ JA ☒ NEIN
22.	Das Mdoc-Lesegerät sendet während der Geräteinteraktion über ein NFC Negotiated Handover eine ReaderEngagement-Struktur als Teil der Handover Request Message.	☐ JA ☒ NEIN
23.	Das Mdoc-Lesegerät richtet ein Time-out für den Zeitraum zwischen der Transaktionsinitialisierung und dem Empfang der Geräteinteraktionsdaten ein.	☐ JA ☒ NEIN
24.	Bei Auswahl von JA geben Sie die Dauer des Time-outs (in Sekunden) an.	xx Sekunden
25.	Das Mdoc-Lesegerät richtet ein Time-out für den Zeitraum zwischen dem Empfang der Geräteinteraktionsdaten und der erfolgreichen Einrichtung einer Geräteabrufverbindung ein.	☐ JA ☒ NEIN
26.	Bei Auswahl von JA geben Sie die Dauer des Time-outs (in Sekunden) an.	xx Sekunden

A.1.3 Für Sicherheitsmechanismus-Testfälle

Nr.	Erklärungen zur Konformität der Implementierung für Sicherheitsmechanismus-Testfälle	
27.	Das Mdoc-Lesegerät unterstützt die Authentifizierung von Mdoc-Lesegeräten.	☒ JA ☐ NEIN
28.	Bei Auswahl von JA steht während der Prüfung eine Test-CRL für alle vom Mdoc-Lesegerät verwendeten Authentifizierungszertifikate für Mdoc-Lesegeräte zur Verfügung.	☒ JA ☐ NEIN
29.	Bei Auswahl von JA besitzt die Zertifizierungsstelle, die alle vom Mdoc-Lesegerät verwendeten Authentifizierungszertifikate des Mdoc-Lesegeräts signiert hat, einen OCSP-Dienst.	☐ JA ☒ NEIN
30.	Bei Auswahl von JA steht während der Prüfung ein Test-OCSP-Responder für alle vom Mdoc-Lesegerät verwendeten Authentifizierungszertifikate für Mdoc-Lesegeräte zur Verfügung.	☐ JA ☒ NEIN
31.	Bei Auswahl von JA welche Kurve verwendet das Mdoc-Lesegerät für die Authentifizierung von Mdoc-Lesegeräten? Wählen Sie eine Antwort aus.	☒ Kurve P-256 ☒ Kurve P-384 ☒ Kurve P-521 ☒ Ed25519 ☒ Ed448 ☒ brainpoolP256r1 ☒ brainpoolP320r1 ☒ brainpoolP384r1 ☒ brainpoolP512r1
32.	Das Mdoc-Lesegerät unterstützt den Austausch von mehr als einer Mdoc-Anfrage und -Antwort zur Geräteabfrage beim Mdoc in einer einzigen Sitzung.	☐ JA ☒ NEIN



fime.com

33.	Das Mdoc-Lesegerät unterstützt den Austausch von mehr als einer Anfrage und Antwort zur Serverabfrage bei der Infrastruktur der ausstellenden Zertifizierungsstelle in einer einzigen Sitzung.	☐ JA ☒ NEIN
34.	Das Mdoc-Lesegerät unterstützt den Abruf von OCSP-Informationen (sofern vorhanden) bei der Verifizierung eines TLS-Serverzertifikats. [1]	☐ JA ☒ NEIN
35.	Das Mdoc-Lesegerät fragt OCSP-Statusinformationen für das Serverzertifikat im TLS-Handshake ab [1]	☐ JA ☒ NEIN
36.	Das Mdoc-Lesegerät unterstützt TLS v 1.3. [1]	☐ JA ☒ NEIN
37.	Das Mdoc-Lesegerät unterstützt die Authentifizierung von TLS-Clients	☐ JA ☒ NEIN
38.	Bei Auswahl von JA steht während der Prüfung eine Test-CRL für alle vom Mdoc-Lesegerät verwendeten TLS-Clientzertifikate zur Verfügung	☐ JA ☒ NEIN
39.	Falls unter Punkt 34 ja ausgewählt wird, besitzt die Zertifizierungsstelle, die alle vom Mdoc-Lesegerät verwendeten TLS-Clientauthentifizierungszertifikate signiert hat, einen OCSP-Dienst.	☐ JA ☒ NEIN
40.	Bei Auswahl von JA steht während der Prüfung ein Test-OCSP-Responder für alle vom Mdoc-Lesegerät verwendeten TLS-Clientauthentifizierungszertifikate zur Verfügung.	☐ JA ☒ NEIN
41.	Wie viele Sekunden beträgt das vom Mdoc-Lesegerät eingerichtete Time-out für die Beendigung der Sitzung?	300 Sekunden

[1] Diese Aussage trifft nur zu, falls das Mdoc-Lesegerät eine Serverabfrage über WebAPI unterstützt

CONSORCIO EMDOC CONSORCIO Santo Domingo, R.D.

fime.com

744

I, notary representative, hereby certify that this document is a true copy of a pdf file.

Munich, this 15.01.2025

[Notary's seal]

[Signature]

Dr Christian Linke,

notary representative of

Dr Bernhard Schaub
Notary Public in Munich,
Federal Republic of Germany
(commission expires: October 31, 2032)

The authenticity of the preceding signature of Dr Christian Linke, notary representative, and the seal hereto affixed is hereby certified.
It is also certified that the above-mentioned person was authorized to carry out this official act.

Munich, January 16, 2025
The President of the Munich Regional Court I [*Landgericht*]
By proxy

[Illegible signature]

Lea Adelsberger
Court Employee

[Round seal of the Munich Regional Court, Bavaria]

CONSORCIO EMDOC CONSORCIO Santo Domingo, R D

Als vom Präsidenten des Landgerichts München I öffentlich bestellter und allgemein beeidigter Übersetzer für die englische Sprache bestätige ich: Vorstehende Übersetzung des mir in englischer Sprache als beglaubigte Abschrift vorgelegten Dokuments ist richtig und vollständig.

München, den 30. Januar 2025

In my capacity as a public certified translator for the English language, duly commissioned and sworn by the President of the Regional Court I of Munich, Bavaria, I hereby certify the above to be a true and correct translation of the English document presented to me as a certified copy.

Munich, January 30, 2025

Öffentlich bestellter und beeidigter Übersetzer für die englische Sprache
Patrick Hampp
Annelies-Kuppel-Allee 20
85540 Haar

Unterschrift u. Stempel:
Signature & stamp:

Patrick Hampp | Annelies-Kuppel-Allee 20 | 85540 Haar

CONSORCIO EMDOC CONSULTO
Santo Domingo, R D

fime

Certified Copy

746

Veridos
Nicholas Larter
Oranienstraße 91, Berlin, Germany 10969

27th August 2024

Subject: Confirmation of conformity of Android-based VO CheckID Version 1.0.12[12] with ISO/IEC 18013-5:2021

Dear Mr. Larter,

This letter serves to confirm that the abovementioned mDL reader was tested by FIME and found to be compliant with ISO/IEC 18013-5:2021 as of the date of this letter.

The test scope included testing the mDL reader on its interface to an mDL, by executing the test cases listed in the latest draft version of ISO/IEC 18013-6. Testing was limited to the features supported by the mDL reader, as indicated in the Implementation Conformance Statement in the Appendix to this letter. Details of the application under test, the test environment, and the test devices used for testing can be found on the next page.

As a reminder, the correct functioning of the mDL reader is dependent on several factors in its operational environment. Veridos is solely and fully responsible for the conformity of the mDL reader to all applicable standards, specifications, and requirements.

The number of the Test Report corresponding to this letter is FIME_eID_Veridos_Android_01. This report contains the full overview of executed test cases and all test results.

Yours sincerely,

FIME

David Bakker
Technical Lead

CONSORCIO EMDOC Santo Domingo, R.D.

FIME Services North America Inc, 1945 The Exchange, Suite 200 SE, Atlanta, GA 30339, United States

mDL implementation scope

System Under Test

Application name and version	VD CheckID Version 1.0.12(12)
Date of receipt of application	2024-07-23

Implementation Conformance Statement Summary

Device engagement technologies	QR code NFC Static Handover NFC Negotiated Handover
Device retrieval technologies	BLE in mdoc central client mode BLE in mdoc peripheral server mode NFC
Server retrieval technologies	None
Security mechanisms for device retrieval	Session encryption, issuer data authentication, mdoc ECDSA/EdDSA authentication, mdoc reader authentication

Test Environment

Standard	ISO/IEC 18013-5:2021
Test Case Specification	FIME mDL Reader Test Case Specification
Test Suite	FIME mDL Reader Test Suite v1.4.0
mDL Test App	mdlreadertestapp-1.4.0.apk
Test device on which the mDL Test App is installed	Samsung Galaxy S20+ 5G
OS version of the test device on which the mDL Test App is installed	Android 12

Test Devices and Platform

Device attachment type	Samsung Galaxy S24	Google Pixel 3a
OS version	Android 14	Android 12

CONSORCIO EMDOC
EMDOC CONSORCIO
Santo Domingo, R.D.

7 1/2

A.1 Implementation conformance statement

The Implementation Conformance Statements below were provided to FIME by Veridos and have been used to determine which test cases to execute.

The ICS version used by Veridos is v1.6.

A.1.1 General information

mDL owner	
Application owner Name	Veridos
Address	Oranienstraße 91, Berlin, Germany 10969
City	Berlin
State	Berlin
Zip Code / Postal Code	10969
Country	Germany
Contact Name	Nicholas Larter
Contact Title	Senior Solutions Manager
Contact Email Address	nick.larter@veridos.com
Contact Phone Number	+49 1525 1334198

#	mDL reader General Information	
-	Reader Application name and version	VD CheckID Version 1.0.12(12)
-	Minimum version of Android supported	Android 12



1.	Specify which DocType(s) the mDL reader supports	1
2.	For each DocType, specify which namespace(s) the mDL reader supports.	org.iso.18013.5.1.mdl
3.	For each namespace, specify the identifiers of all data elements that can be requested by the mDL reader.	family_name given_name birth_date document_number driving_privileges issue_date expiry_date issuing_authority issuing_country portrait un_distinguishing_sign sex height weight eye_colour hair_colour age_in_years age_birth_year birth_place nationality portrait_capture_date resident_address resident_city resident_state resident_postal_code resident_country signature_usual_mark family_name_national_character given_name_national_character age_over_18 age_over_19 age_over_20 age_over_21 age_over_22 age_over_23 age_over_24 age_over_25 age_over_26
4.	mDL reader is able to request multiple documents in a single DeviceRequest message.[1]	☐YES ☒NO
5.	mDL reader is able to request multiple documents in a single ServerRequest message.[1]	☐YES ☒NO

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.
lmle.com

6.	mDL reader is able to request the issuing_jurisdiction data element from namespace org.iso.18013.5.1	☐YES ☒NO
7.	mDL reader is able to request the age_over_NN data element from namespace org.iso.18013.5.1	☒YES ☐NO
8.	mDL reader is able to request the issuing_country data element from namespace org.iso.18013.5.1	☒YES ☐NO

A.1.2 For technology test cases

#	ICS statements for Technologies Test cases	
9.	mdoc reader supports device engagement using NFC Static Handover. [4]	☒YES ☐NO
10.	mdoc reader supports device engagement using NFC Negotiated Handover. [4]	☒YES ☐NO
11.	mdoc reader supports device engagement using a QR code. [4]	☒YES ☐NO
12.	mdoc reader supports device retrieval using NFC. [4]	☒YES ☐NO
13.	mdoc reader supports device retrieval using BLE in mdoc central client mode. [4]	☒YES ☐NO
14.	mdoc reader supports device retrieval using BLE in mdoc peripheral server mode. [4]	☒YES ☐NO
15.	mdoc reader supports device retrieval using BLE version 5.0 (or above) and LE 2M PHY.	☐YES ☒NO
16.	mdoc reader supports device retrieval using Wi-Fi Aware.	☐YES ☒NO
17.	mdoc reader supports server retrieval using OIDC	☐YES ☒NO
18.	mdoc reader supports server retrieval using WebAPI.	☐YES ☒NO
19.	mdoc reader supports extended-length APDUs for device retrieval using NFC.	☒YES ☐NO
20.	mdoc reader supports the L2CAP transmission profile if it is acting as the GATT client for device retrieval using BLE.	☐YES ☒NO

[1] If this is set to YES, the mDL reader should support at least two different DocTypes.
[3] This statement is only applicable if the mDL reader supports server retrieval using WebAPI.
[4] If this statement is set to YES, the mDL reader should support at least two different DocTypes.
[4] Note this is mandatory to support for mDL readers, but optional for mdoc readers in general.



21.	mdoc reader supports the L2CAP transmission profile if it is acting as the GATT server for device retrieval using BLE.	☐YES ☒NO
22.	mdoc reader sends a ReaderEngagement structure as part of the Handover Request Message during device engagement using NFC Negotiated Handover.	☐YES ☒NO
23.	mdoc reader implements a time-out for the time between the transaction initialization and receiving device engagement data.	☐YES ☒NO
24.	If yes, indicate how long is the time-out (in seconds).	xx seconds
25.	mdoc reader implements a time-out for the time between receiving device engagement data and the successful set-up of a device retrieval connection.	☐YES ☒NO
26.	If yes, indicate how long is the time-out (in seconds).	xx seconds

A.1.3 For security mechanism test cases

#	ICS statements for Security Mechanisms test cases	
27.	mdoc reader supports mdoc reader authentication	☒YES ☐NO
28.	If yes, a test CRL for all mdoc reader authentication certificates used by the mdoc reader is available during testing	☒YES ☐NO
29.	If yes, the CA that signed all mdoc reader authentication certificates used by the mdoc reader has an OCSP service.	☐YES ☒NO
30.	If yes, a test OCSP Responder for all mdoc reader authentication certificates used by the mdoc reader is available during testing.	☐YES ☒NO
31.	If yes, which curve does the mdoc reader use for mdoc reader authentication? Tick one.	☒ Curve P-256 ☒ Curve P-384 ☒ Curve P-521 ☒ Ed25519 ☒ Ed448 ☒ brainpoolP256r1 ☒ brainpoolP320r1 ☒ brainpoolP384r1 ☒ brainpoolP512r1
32.	mdoc reader supports exchanging more than one device retrieval mdoc request and response with the mdoc in a single session.	☐YES ☒NO
33.	mdoc reader supports exchanging more than one server retrieval request and response with the issuing authority infrastructure in a single session.	☐YES ☒NO
34.	mdoc reader supports retrieving OCSP information, if available when verifying a TLS server certificate. [1]	☐YES ☒NO

[1] This statement is only applicable if the mdoc reader supports server retrieval using WebAPI.



lime.com

35.	mdoc reader requests OCSP status information for the server certificate in the TLS handshake [3]	☐YES ☒NO
36.	mdoc reader supports TLS v 1.3. [4]	☐YES ☒NO
37.	mdoc reader supports TLS Client Authentication.	☐YES ☒NO
38.	If yes, a test CRL for all TLS Client certificates used by the mdoc reader is available during testing	☐YES ☒NO
39.	If yes to #34, the CA that signed all TLS Client authentication certificates used by the mdoc reader has an OCSP service.	☐YES ☒NO
40.	If yes, a test OCSP Responder for all TLS Client authentication certificates used by the mdoc reader is available during testing.	☐YES ☒NO
41.	How many seconds is the time-out period for session termination implemented by the mdoc reader?	300 seconds

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.
emdoc.com

753

I, notary representative, hereby certify that this document is a true copy of a pdf-file.

Munich, this 15.01.2025

Dr. Christian Linke,
notary representative of
Dr. Bernhard Schaub
Notary Public in Munich,
Federal Republic of Germany
(commission expires: October 31, 2032)

Die Echtheit vorstehender Unterschrift des Notarassessors Dr. Christian Linke und die Echtheit des beigedrückten Dienstsiegels werden hiermit bestätigt.
Zugleich wird bescheinigt, dass der Vorgenannte zur Vornahme der Amtshandlung befugt war.

München, 16. Januar 2025
Die Präsidentin des Landgerichts München I
Im Auftrag

Ilse Adelsberger
Justizsekretärin

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

754

Übersetzt, beglaubigt und beeidigter Übersetzer für die spanische Sprache
Susanne Bernhardt
Ravensburger Ring 15
81243 München

Übersetzt, beglaubigt und beeidigter Übersetzer für die spanische Sprache
Patrick Hampp
Amalie-Nuppel-Allee 20
82340 Haar

EMBAJADA DE LA REPÚBLICA DOMINICANA
EN ALEMANIA
SECCIÓN CONSULAR

CERTIFICO, que la firma que aparece al pie de esta documentación es la del/ de la Sr./a. Abdelbagen - Justiz- u. Rechtsanw.
CIUDAD München y que es la misma que acostumbra a usar en todos sus actos y la cual es de su entera fé y crédito.
FECHA 12-02-2025

EMBAJADA DE LA REPÚBLICA DOMINICANA BERLIN ALEMANIA

HEIDI TAVERAS
CONSEJERA

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

755

Traducción jurada del alemán

Traducción jurada del inglés

[Logotipo de la empresa fime] Copia notarial

Veridos
Nicholas Larter
Oranienstraße 91, 10969 Berlín

27 de agosto de 2024

Asunto: Confirmación de la conformidad del VD CheckID basado en iOS, versión 1.0.6 (6) con la norma ISO/IEC 18013-5:2021

Estimado Sr. Larter:

Nos dirigimos a usted para confirmarle que el lector mDL mencionado anteriormente ha sido probado por FIME y ha resultado ser conforme con la norma ISO/IEC 18013--5:2021 a partir de la fecha de esta carta.

Parte de las pruebas consistió en comprobar la interfaz del lector mDL con un mDL mediante la ejecución de los casos de prueba enumerados en la última versión del borrador de la norma ISO/IEC 18013--6. Solo se realizaron aquellas pruebas compatibles con las funciones del lector mDL, tal y como se especifica en la Declaración de Conformidad de la Implementación adjunta a esta carta. Para más información sobre la aplicación probada, el entorno de prueba y el equipo utilizado para la prueba, consulte la página siguiente.

Debe tenerse en cuenta que el correcto funcionamiento del lector mDL depende de diversos factores dentro de su entorno operativo. Veridos es el único y pleno responsable de la conformidad del lector mDL con todas las normas, especificaciones y requisitos aplicables.

El informe de pruebas que acompaña a esta carta lleva el número FIME_eID_Veridos_iOS_01. Este protocolo contiene una descripción completa de los casos de prueba ejecutados y todos los resultados de las pruebas.

Atentamente

FIME
[Firma]
David Bakker
Director técnico

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

Ámbito de aplicación de mDL

Sistema probado

Nombre y versión de la aplicación	VD CheckID Versión 1.0.6(6)
Aplicación recibida el	23 de julio de 2024

Resumen de la declaración de conformidad de la aplicación

Tecnologías para la interacción con el dispositivo	Código QR NFC Static Handover NFC Negotiated Handover
Tecnologías para la consulta de dispositivos	BLE en el modo cliente central del Mdoc BLE en el modo servidor periférico del Mdoc NFC
Tecnologías para la consulta del servidor	Ninguna
Mecanismos de seguridad para la consulta del dispositivo	Cifrado de las sesiones, autentificación de los datos del emisor, autentificación Mdoc ECDSA/EdDSA, autentificación de los lectores Mdoc

Entorno de prueba

Norma	ISO/IEC 18013-5:2021
Especificación de casos de prueba	Especificación de casos de prueba FIME para el lector mDL
Conjunto de pruebas	FIME Test Suite v1.4.0 para el lector mDL
Aplicación de prueba mDL	mdlreadertestapp-1.4.0.apk
Dispositivo de prueba en el que está instalada la aplicación de prueba mDL	Samsung Galaxy S24
Versión del sistema operativo del dispositivo de prueba en el que está instalada la aplicación de prueba mDL	Android 14

Dispositivos de prueba y plataforma

Marca y tipo de dispositivo	iPhone 15	iPhone SE (2a generación)
Versión del sistema operativo	iOS 17.6.1	iOS 15.5

CONSORCIO EMDOC
EMDOC CONSORCIO
Santo Domingo, R D

A.1 Declaración de conformidad de la implementación

Veridos envió a la FIME las siguientes declaraciones de conformidad de la implementación (Implementation Conformance Statement, ICS). Se han utilizado para determinar los casos de prueba que deben ejecutarse.

Veridos utiliza la versión v1.6 de ICS.

A.1.1 Información general

Propietario de mDL	
Nombre del propietario de la aplicación	Veridos
Dirección	Oranienstraße 91, 10969 Berlin
Ciudad	Berlin
Estado Federal	Berlin
C.P.	10969
País	Alemania
Nombre de la persona de contacto	Nicholas Larter
Cargo	Senior Solutions Manager
Correo electrónico de la persona de contacto	nick.larter@veridos.com
Número de teléfono de la persona de contacto	+49 1525 1334198

N.º	Información general sobre el lector mDL	
-	Nombre y versión de la aplicación del lector	VD CheckID Versión 1.0.6(6)
-	Versión iOS compatible más baja	iOS 15



1.	Especifique qué DocType(s) admite el lector mDL	1
2.	Para cada DocType, especifique qué espacio/s de nombres admite el lector mDL.	org.iso.18013.5.1.mDl
3.	Para cada espacio de nombres, introduzca los identificadores de todos los elementos de datos que pueden ser consultados por el lector mDL.	family_name given_name birth_date document_number driving_privileges issue_date expiry_date issuing_authority issuing_country portrait un_distinguishing_sign sex height weight eye_colour hair_colour age_in_years age_birth_year birth_place nationality portrait_capture_date resident_address resident_city resident_state resident_postal_code resident_country signature_usual_mark family_name_national_character given_name_national_character age_over_18 age_over_19 age_over_20 age_over_21 age_over_22 age_over_23 age_over_24 age_over_25 age_over_26
4.	El lector mDL es capaz de solicitar múltiples documentos en un único mensaje DeviceRequest. [4]	☐ SÍ ☒ NO
5.	El lector mDL es capaz de solicitar múltiples documentos en un único mensaje DeviceRequest. [13]	☐ SÍ ☒ NO

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

6.	El lector mDL puede consultar el elemento de datos «issuing_jurisdiction» del espacio de nombres «org.iso.18013.5.1».	☐ SÍ ☒ NO
7.	El lector mDL puede consultar el elemento de datos «age_over_NN» del espacio de nombres «org.iso.18013.5.1».	☒ SÍ ☐ NO
8.	El lector mDL puede consultar el elemento de datos «issuing_country» del espacio de nombres «org.iso.18013.5.1».	☒ SÍ ☐ NO

A.1.2 Para casos de pruebas de tecnología

N.º	Declaraciones de conformidad de la implementación para los casos de prueba de tecnología	
9.	El lector Mdoc admite la interacción de dispositivos mediante el traspaso estático NFC. [4]	☒ SÍ ☐ NO
10.	El lector Mdoc es compatible con la interacción de dispositivos vía NFC Negotiated Handover. [4]	☒ SÍ ☐ NO
11.	El lector Mdoc admite la interacción de dispositivos mediante un código QR. [4]	☒ SÍ ☐ NO
12 de	El lector Mdoc admite el escaneado de dispositivos mediante NFC. [4]	☒ SÍ ☐ NO
13.	El lector Mdoc admite consultas de dispositivos a través de BLE en el modo de cliente central del Mdoc. [4]	☒ SÍ ☐ NO
14.	El lector Mdoc admite consultas de dispositivos a través de BLE en el modo de servidor periférico del Mdoc. [4]	☒ SÍ ☐ NO
15.	El lector Mdoc admite la consulta de dispositivos mediante BLE versión 5.0 (o superior) y LE 2M PHY.	☐ SÍ ☒ NO
16.	El lector Mdoc admite el sondeo de dispositivos a través de Wi-Fi Aware.	☐ SÍ ☒ NO
17.	El lector Mdoc admite consultas al servidor a través de OIDC	☐ SÍ ☒ NO
18.	El lector Mdoc admite consultas al servidor a través de WebAPI.	☐ SÍ ☒ NO
19.	El lector Mdoc admite APDUs extralargos para consultas de dispositivos a través de NFC.	☒ SÍ ☐ NO
20.	El lector Mdoc admite el perfil de transmisión L2CAP cuando actúa como cliente GATT para la consulta de dispositivos a través de BLE.	☐ SÍ ☒ NO
21.	El lector Mdoc admite el perfil de transmisión L2CAP si actúa como servidor GATT para la consulta de dispositivos a través de BLE.	☐ SÍ ☒ NO
22.	El lector Mdoc envía una estructura ReaderEngagement como parte del mensaje Handover Request Message durante la interacción con el dispositivo a través de [illegible]	☐ SÍ ☒ NO

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD
firme.com

	NFC Negotiated Handover.	
23.	El lector Mdoc establece un Time-out para el periodo entre la inicialización de la transacción y la recepción de los datos de interacción del dispositivo.	☐ SÍ ☒ NO
24.	Si selecciona SÍ, introduzca la duración del Time-out (en segundos).	xx segundos
25.	El lector Mdoc establece un Time-out para el periodo entre la recepción de los datos de interacción del dispositivo y el establecimiento satisfactorio de una conexión de consulta del dispositivo.	☐ SÍ ☒ NO
26.	Si selecciona SÍ, introduzca la duración del Time-out (en segundos).	xx segundos

A.1.3 Para casos de prueba de mecanismos de seguridad

N.º	Declaraciones de conformidad de la implementación para los casos de prueba de mecanismos de seguridad	
27.	El lector Mdoc es compatible con la autenticación de lectores Mdoc.	☒ SÍ ☐ NO
28.	Si se selecciona SÍ, durante la comprobación se dispone de una CRL de prueba para todos los certificados de autenticación de lectores Mdoc utilizados por el lector Mdoc.	☒ SÍ ☐ NO
29.	Si se selecciona SÍ, la autoridad de certificación que ha firmado todos los certificados de autenticación de lectores Mdoc utilizados por el lector Mdoc dispone de un servicio OCSP.	☐ SÍ ☒ NO
30.	Si se selecciona SÍ, se dispone de un OCSP-Responder de prueba durante la comprobación de todos los certificados de autenticación para lectores Mdoc utilizados por el lector Mdoc.	☐ SÍ ☒ NO
31.	Si se selecciona SÍ, ¿qué curva utiliza el lector Mdoc para la autenticación de los lectores Mdoc?	☒ Curva P-256 ☒ Curva P-384 ☒ Curva P-521 ☒ Ed25519 ☒ Ed448 ☒ brainpoolP256r1 ☒ brainpoolP320r1 ☒ brainpoolP384r1 ☒ brainpoolP512r1
32.	El lector de Mdoc admite el intercambio de más de una solicitud y respuesta de Mdoc para la consulta del dispositivo en el Mdoc en una única sesión.	☐ SÍ ☒ NO
33.	El lector Mdoc admite el intercambio de más de una solicitud y respuesta para la consulta del servidor en la infraestructura de la autoridad de certificación emisora en una única sesión.	☐ SÍ ☒ NO
34.	El lector Mdoc admite la recuperación de información OCSP (si está disponible) al verificar un certificado de servidor TLS. [1]	☐ SÍ ☒ NO

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.
fime.com

35.	El lector Mdoc consulta la información de estado OCSP del certificado del servidor en el protocolo de enlace TLS. [5]	☐ SÍ ☒ NO
36.	El lector Mdoc admite TLS v 1.3. [5]	☐ SÍ ☒ NO
37.	El lector Mdoc admite la autenticación de clientes TLS.	☐ SÍ ☒ NO
38.	En caso afirmativo, se dispone de una CRL de prueba durante la prueba para todos los certificados de cliente TLS utilizados por el lector de Mdoc	☐ SÍ ☒ NO
39.	Si se selecciona SÍ en el punto 34, la autoridad de certificación que ha firmado todos los certificados de autenticación de clientes TLS utilizados por el lector Mdoc dispone de un servicio OCSP.	☐ SÍ ☒ NO
40.	Si la respuesta es afirmativa, se dispondrá de un OCSP-Responder de prueba durante las pruebas para todos los certificados de autenticación de cliente TLS utilizados por el lector Mdoc.	☐ SÍ ☒ NO
41.	¿Cuántos segundos dura el Time-out de finalización de sesión establecido por el lector Mdoc?	300 segundos

[1] Si se selecciona SÍ, el lector mDL debe de apoyar por lo menos dos diferentes DocTypes.
[2] Esa declaración sólo es aplicable si el lector mDL apoya consultas al servidor a través de WebAPI.
[3] Si se selecciona SÍ, el lector mDL debe de apoyar por lo menos dos dos diferentes DocTypes.
[4] Por favor tenga en cuenta que eso es mandatorio para apoyar lectores mDL, pero opcional para lectores mdoc en general.
[5] Esa declaración sólo es aplicable si el lector mdoc apoya consultas al servidor a través de WebAPI.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

time.com

762

Yo, representante notarial, certifico que este documento es una copia fiel de un archivo pdf.

En Múnich, a 15/01/2025

[Sello del notario]

[Firma]

Dr. Christian Linke,

representante notarial de

Dr. Bernhard Schaub
Notario en Múnich,
República Federal de Alemania
(el mandato expira el 31 de octubre de 2032)

Por la presente se certifica la autenticidad de la firma precedente del Dr. Christian Linke, representante notarial, y del sello aquí estampado.
Asimismo, se certifica que la persona arriba mencionada estaba autorizada para llevar a cabo este acto oficial.

Múnich, 16 de enero de 2025
El Presidente del Tribunal Regional I de Múnich [Landgericht]
Por poder

[Firma ilegible]

Lea Adelsberger
Empleada del Tribunal

[Sello redondo del Tribunal Regional de Múnich, Baviera]

CONSORCIO EMDOC
EMDOC CONSORCIO
Santo Domingo

763

Als in Bayern öffentlich bestellte und allgemein beeidigte Dolmetscherin für die englische und spanische Sprache bestätige ich: Vorstehende Übersetzung des mir in englischer Sprache als beglaubigte Abschrift vorgelegten Dokuments ist richtig und vollständig.

München, den 01. Februar 2025

Como traductora jurada y nombrada públicamente para los idomas alemán, inglés y español en Baviera, confirmo que la traducción que precede de la copia certificada del documento que se me ha presentado en lengua inglesa es correcta y completa.

Múnich, a 1 de febrero del 2025

Unterschrift und Stempel:

Firma y sello:

Öffentlich bestellte und beeidigte Übersetzerin für die spanische Sprache
Susanne Bernhardt
Ravensburger Ring 18
81243 München

Susanne Bernhardt – Ravensburger Ring 18 – 81243 München

Die Echtheit vorstehender Unterschrift der Übersetzerin Susanne Bernhardt wird hiermit bestätigt.
Zugleich wird bescheinigt, dass die Vorgenannte öffentlich bestellte und allgemein beeidigte Übersetzerin für die spanische Sprache ist.

München, 07. Februar 2025
Die Präsidentin des Landgerichts München I
Im Auftrag

Justizsekretärin

EMBAJADA DE LA REPÚBLICA DOMINICANA

CERTIFICO, que la

CONSORCIO EMDOC

Santo Domingo, R.D.

Beglaubigte Übersetzung aus dem Englischen

764

[Firmenlogo von fime] Beglaubigte Abschrift

Veridos
Nicholas Larter
Cranienstraße 91, 10969 Berlin

27. August 2024

Betreff: Bestätigung der Konformität der auf iOS basierenden VD CheckID, Version 1.0.6 (6) mit ISO/IEC 18013-5:2021

Sehr geehrter Herr Larter,

mit diesem Schreiben bestätigen wir, dass das oben genannte mDL-Lesegerät von FIME getestet und im Ergebnis festgestellt wurde, dass es mit Stand zum Datum dieses Schreibens der Norm ISO/IEC 18013-5:2021 entspricht.

Teil des Testumfangs war die Prüfung des mDL-Lesegeräts auf seiner Schnittstelle zu einem mDL durch Ausführung der in der neuesten Entwurfsfassung von ISO/IEC 18013-6 aufgeführten Testfälle. Die Prüfung bezog sich nur auf vom mDL-Lesegerät unterstützte Funktionen, wie in der diesem Schreiben beigefügten Erklärung zur Konformität der Implementierung angegeben. Nähere Informationen zu der getesteten Anwendung, der Testumgebung und den für den Test verwendeten Prüfgeräten sind der folgenden Seite zu entnehmen.

Es wird darauf hingewiesen, dass die ordnungsgemäße Funktion des mDL-Lesegeräts von verschiedenen Faktoren innerhalb ihrer Betriebsumgebung abhängt. Für die Konformität des mDL-Lesegeräts mit allen geltenden Normen, Spezifikationen und Anforderungen trägt Veridos die alleinige und volle Verantwortung.

Das zu diesem Schreiben gehörende Prüfprotokoll trägt die Nummer FIME_eID_Veridos_iOS_01. Dieses Protokoll enthält eine vollständige Übersicht der ausgeführten Testfälle und aller Testergebnisse.

Mit freundlichen Grüßen
[Unterschrift]

FIME

David Bakker
Technischer Leiter

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

1

765

mDL-Implementierungsumfang

Getestetes System

Bezeichnung und Version der Anwendung	VD CheckID Version 1.0.6(6)
Anwendung erhalten am	23. Juli 2024

Zusammenfassung der Erklärung zur Konformität der Implementierung

Technologien zur Gerätebindung	QR-Code NFC Static Handover NFC Negotiated Handover
Technologien zur Geräteabfrage	BLE im zentralen Client-Modus des Mdoc BLE im Peripherieserver-Modus des Mdoc NFC
Technologien zur Serverabfrage	Keine
Schutzmechanismen für die Geräteabfrage	Verschlüsselung von Sitzungen, Authentifizierung von Ausstellerdaten, Mdoc ECDSA-/EdDSA-Authentifizierung, Authentifizierung von Mdoc-Lesegeräten

Testumgebung

Standard	ISO/IEC 18013-5:2021
Testfallspezifikation	FIME Testfallspezifikation für mDL-Lesegerät
Testsuite	FIME Test Suite v1.4.0 für mDL-Lesegerät
mDL-Testapp	mdlreadertestapp-1.4.0.apk
Prüfgerät, auf dem die mDL-Testapp installiert ist	Samsung Galaxy S24
Version des Betriebssystems auf dem Prüfgerät, auf dem die mDL-Testapp installiert ist	Android 14

Prüfgeräte und -plattform

Marke und Typ des Geräts	iPhone 15	iPhone SE (2. Generation)
Version des Betriebssystems	iOS 17.6.1	iOS 15.5

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

fime.com

764

A.1 Erklärung zur Konformität der Implementierung

Die folgenden Erklärungen zur Konformität der Implementierung (Implementation Conformance Statement, ICS) wurden FIME von Veridos vorgelegt. Anhand dieser wurde ermittelt, welche Testfälle auszuführen sind.

Veridos verwendet die ICS-Version v1.6.

A.1.1 Allgemeine Informationen

mDL-Eigentümer	
Name des Eigentümers der Anwendung	Veridos
Anschrift	Oranienstraße 91, 10969 Berlin
Stadt	Berlin
Bundesland	Berlin
PLZ	10969
Land	Deutschland
Name des Ansprechpartners	Nicholas Larter
Positionsbezeichnung	Senior Solutions Manager
E-Mail-Adresse des Ansprechpartners	nick.larter@veridos.com
Telefonnummer des Ansprechpartners	+49 1525 1334198

Nr.	Allgemeine Informationen zum mDL-Lesegerät	
-	Bezeichnung und Version der Lesegeräteanwendung	VD CheckID Version 1.0.6(6)
-	Niedrigste unterstützte iOS-Version	iOS 15

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo

fime.com

1.	Geben Sie an, welche DocType(s) vom mDL-Lesegerät unterstützt werden	1
2.	Geben Sie für jeden DocType an, welche Namespace(s) vom mDL-Lesegerät unterstützt werden.	org.iso.18013.5.1.mdl
3.	Geben Sie für jeden Namespace die Kennungen aller Datenelemente an, die vom mDL-Lesegerät abgefragt werden können.	family_name given_name birth_date document_number driving_privileges issue_date expiry_date issuing_authority issuing_country portrait un_distinguishing_sign sex height weight eye_colour hair_colour age_in_years age_birth_year birth_place nationality portrait_capture_dat e resident_address resident_city resident_state resident_postal_code resident_country signature_usual_mark family_name_national_character given_name_national_character age_over_18 age_over_19 age_over_20 age_over_21 age_over_22 age_over_23 age_over_24 age_over_25 age_over_26
4.	Das mDL-Lesegerät ist in der Lage, mehrere Dokumente in einer einzigen DeviceRequest-Meldung abzufragen. [1]	☐ JA ☒ NEIN

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD
fime.com

5.	Das mDL-Lesegerät ist in der Lage, mehrere Dokumente in einer einzigen ServerRequest-Meldung abzufragen.[2] [3]	☐ JA ☒ NEIN
6.	Das mDL-Lesegerät ist in der Lage, das „issuing_jurisdiction"-Datenelement vom Namespace „org.iso.18013.5.1" abzufragen	☐ JA ☒ NEIN
7.	Das mDL-Lesegerät ist in der Lage, das „age_over_NN"-Datenelement vom Namespace „org.iso.18013.5.1" abzufragen	☒ JA ☐ NEIN
8.	Das mDL-Lesegerät ist in der Lage, das „issuing_country"-Datenelement vom Namespace „org.iso.18013.5.1" abzufragen	☒ JA ☐ NEIN

A.1.2 Für Technologie-Testfälle

Nr.	Erklärungen zur Konformität der Implementierung für Technologie-Testfälle	
9.	Das Mdoc-Lesegerät unterstützt Geräteinteraktion über NFC Static Handover. [4]	☒ JA ☐ NEIN
10.	Das Mdoc-Lesegerät unterstützt Geräteinteraktion über NFC Negotiated Handover. [3]	☒ JA ☐ NEIN
11.	Das Mdoc-Lesegerät unterstützt Geräteinteraktion über einen QR-Code. [4]	☒ JA ☐ NEIN
12.	Das Mdoc-Lesegerät unterstützt Geräteabfrage über NFC. [3]	☒ JA ☐ NEIN
13.	Das Mdoc-Lesegerät unterstützt Geräteabfrage über BLE im zentralen Client-Modus des Mdoc. [3]	☒ JA ☐ NEIN
14.	Das Mdoc-Lesegerät unterstützt Geräteabfrage über BLE im Peripherieserver-Modus des Mdoc. [3]	☒ JA ☐ NEIN
15.	Das Mdoc-Lesegerät unterstützt Geräteabfrage über BLE Version 5.0 (oder höher) und LE 2M PHY.	☐ JA ☒ NEIN
16.	Das Mdoc-Lesegerät unterstützt Geräteabfrage über Wi-Fi Aware.	☐ JA ☒ NEIN
17.	Das Mdoc-Lesegerät unterstützt Serverabfrage über OIDC	☐ JA ☒ NEIN
18.	Das Mdoc-Lesegerät unterstützt Serverabfrage über WebAPI	☐ JA ☒ NEIN
19.	Das Mdoc-Lesegerät unterstützt überlange APDUs für die Geräteabfrage über NFC.	☒ JA ☐ NEIN

[1] Falls hier JA ausgewählt wird, sollte das mDL-Lesegerät mindestens zwei verschiedene DocTypes anfragen können.
[2] Diese Aussage trifft nur zu, falls das mDL-Lesegerät Serverabfragen über WebAPI unterstützt.
[3] Falls hier JA ausgewählt wird, sollte das mDL-Lesegerät mindestens zwei verschiedene DocTypes unterstützen.
[4] Dies ist zur Unterstützung von mDL-Lesegeräten obligatorisch, jedoch optional für Mdoc-Lesegeräte, die anderen Zwecken dienen.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

20.	Das Mdoc-Lesegerät unterstützt das Übermittlungsprofil L2CAP, wenn es als GATT-Client für die Geräteabfrage über BLE fungiert.	☐ JA ☒ NEIN
21.	Das Mdoc-Lesegerät unterstützt das Übermittlungsprofil L2CAP, wenn es als GATT-Server für die Geräteabfrage über BLE fungiert.	☐ JA ☒ NEIN
22.	Das Mdoc-Lesegerät sendet während der Geräteinteraktion über ein NFC Negotiated Handover eine ReaderEngagement-Struktur als Teil der Handover Request Message	☐ JA ☒ NEIN
23.	Das Mdoc-Lesegerät richtet ein Time-out für den Zeitraum zwischen der Transaktionsinitialisierung und dem Empfang der Geräteinteraktionsdaten ein.	☐ JA ☒ NEIN
24.	Bei Auswahl von JA geben Sie die Dauer des Time-outs (in Sekunden) an.	xx Sekunden
25.	Das Mdoc-Lesegerät richtet ein Time-out für den Zeitraum zwischen dem Empfang der Geräteinteraktionsdaten und der erfolgreichen Einrichtung einer Geräteabrufverbindung ein.	☐ JA ☒ NEIN
26.	Bei Auswahl von JA geben Sie die Dauer des Time-outs (in Sekunden) an.	xx Sekunden

A.1.3 Für Sicherheitsmechanismus-Testfälle

Nr.	Erklärungen zur Konformität der Implementierung für Sicherheitsmechanismus-Testfälle	
27.	Das Mdoc-Lesegerät unterstützt die Authentifizierung von Mdoc-Lesegeräten.	☒ JA ☐ NEIN
28.	Bei Auswahl von JA steht während der Prüfung eine Test-CRL für alle vom Mdoc-Lesegerät verwendeten Authentifizierungszertifikate für Mdoc-Lesegeräte zur Verfügung	☒ JA ☐ NEIN
29.	Bei Auswahl von JA besitzt die Zertifizierungsstelle, die alle vom Mdoc-Lesegerät verwendeten Authentifizierungszertifikate des Mdoc-Lesegeräts signiert hat, einen OCSP-Dienst.	☐ JA ☒ NEIN
30.	Bei Auswahl von JA steht während der Prüfung ein Test-OCSP-Responder für alle vom Mdoc-Lesegerät verwendeten Authentifizierungszertifikate für Mdoc-Lesegeräte zur Verfügung.	☐ JA ☒ NEIN
31.	Bei Auswahl von JA welche Kurven verwendet das Mdoc-Lesegerät für die Authentifizierung von Mdoc-Lesegeräten?	☒ Kurve P-256 ☒ Kurve P-384 ☒ Kurve P-521 ☒ Ed25519 ☒ Ed448 ☒ brainpoolP256r1 ☒ brainpoolP320r1 ☒ brainpoolP384r1 ☒ brainpoolP512r1
32.	Das Mdoc-Lesegerät unterstützt den Austausch von mehr als einer Mdoc-Anfrage und -Antwort zur Geräteabfrage beim Mdoc in einer einzigen Sitzung.	☐ JA ☒ NEIN



33.	Das Mdoc-Lesegerät unterstützt den Austausch von mehr als einer Anfrage und Antwort zur Serverabfrage bei der Infrastruktur der ausstellenden Zertifizierungsstelle in einer einzigen Sitzung.	☐ JA ☒ NEIN
34.	Das Mdoc-Lesegerät unterstützt den Abruf von OCSP-Informationen (sofern vorhanden) bei der Verifizierung eines TLS-Serverzertifikats. [5]	☐ JA ☒ NEIN
35.	Das mdoc-Lesegerät fragt OCSP-Statusinformationen für das Serverzertifikat im TLS-Handshake ab [5]	☐ JA ☒ NEIN
36.	Das Mdoc-Lesegerät unterstützt TLS v 1.3. [5]	☐ JA ☒ NEIN
37.	Das Mdoc-Lesegerät unterstützt die Authentifizierung von TLS-Clients.	☐ JA ☒ NEIN
38.	Falls ja, steht während der Prüfung eine Test-CRL für alle vom Mdoc-Lesegerät verwendeten TLS-Clientzertifikate zur Verfügung	☐ JA ☒ NEIN
39.	Falls unter Punkt 34 ja ausgewählt wird, besitzt die Zertifizierungsstelle, die alle vom Mdoc-Lesegerät verwendeten TLS-Clientauthentifizierungszertifikate signiert hat, einen OCSP-Dienst.	☐ JA ☒ NEIN
40.	Falls die Antwort Ja lautet, steht während der Tests ein Test-OCSP-Responder für alle vom Mdoc-Lesegerät verwendeten TLS-Clientauthentifizierungszertifikate zur Verfügung.	☐ JA ☒ NEIN
41.	Wie viele Sekunden beträgt das vom Mdoc-Lesegerät eingerichtete Time-out für die Beendigung der Sitzung?	300 Sekunden

[5] Diese Aussage trifft nur zu, falls das Mdoc-Lesegerät eine Serverabfrage über WebAPI unterstützt.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

fmw.com

771

I, notary representative, hereby certify that this document is a true copy of a pdf file.

Munich, this 15.01.2025

[Notary's seal]

[Signature]

Dr Christian Linke,

notary representative of

Dr Bernhard Schaub
Notary Public in Munich,
Federal Republic of Germany
(commission expires: October 31, 2032)

The authenticity of the preceding signature of Dr Christian Linke, notary representative, and the seal hereto affixed is hereby certified.
It is also certified that the above-mentioned person was authorized to carry out this official act.

Munich, January 16, 2025
The President of the Munich Regional Court I (*Landgericht*)
By proxy

[Illegible signature]

Lea Adelsberger
Court Employee

[Round seal of the Munich Regional Court, Bavaria]

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

772

Als vom Präsidenten des Landgerichts München I öffentlich bestellter und allgemein beeidigter Übersetzer für die englische Sprache bestätige ich: Vorstehende Übersetzung des mir in englischer Sprache als beglaubigte Abschrift vorgelegten Dokuments ist richtig und vollständig.

München, den 30. Januar 2025

In my capacity as a public certified translator for the English language, duly commissioned and sworn by the President of the Regional Court I of Munich, Bavaria, I hereby certify the above to be a true and correct translation of the English document presented to me as a certified copy.

Munich, January 30, 2025

Unterschrift u. Stempel:
Signature & stamp:

Patrick Hampp | Annelies-Kupper-Allee 20 | 85540 Haar

fime

Certified Copy

773

Veridos
Nicholas Larter
Oranienstraße 91, Berlin, Germany 10969

27th August 2024

Subject: Confirmation of conformity of iOS-based VD CheckID Version 1.0.6(6) with ISO/IEC 18013-5:2021

Dear Mr. Larter,

This letter serves to confirm that the abovementioned mDL reader was tested by FIME and found to be compliant with ISO/IEC 18013-5:2021 as of the date of this letter.

The test scope included testing the mDL reader on its interface to an mDL, by executing the test cases listed in the latest draft version of ISO/IEC 18013-6. Testing was limited to the features supported by the mDL reader, as indicated in the Implementation Conformance Statement in the Appendix to this letter. Details of the application under test, the test environment, and the test devices used for testing can be found on the next page.

As a reminder, the correct functioning of the mDL reader is dependent on several factors in its operational environment. Veridos is solely and fully responsible for the conformity of the mDL reader to all applicable standards, specifications, and requirements.

The number of the Test Report corresponding to this letter is FIME_eID_Veridos_iOS_01. This report contains the full overview of executed test cases and all test results.

Yours sincerely,

FIME

David Bakker
Technical Lead

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo R.D.

mDL implementation scope

System Under Test

Application name and version	VD CheckID Version 1.0.6(6)
Date of release of application	2024-07-23

Implementation Conformance Statement Summary

Device engagement technologies	QR code NFC Static Handover NFC Negotiated Handover
Device retrieval technologies	BLE is mdoc central client mode BLE is mdoc peripheral server mode NFC
Server retrieval technologies	None
Security mechanisms for device retrieval	Session encryption, issuer data authentication, mdoc ECDSA/EdDSA authentication, mdoc reader authentication

Test Environment

Standard	ISO/IEC 18013-5:2021
Test case specification	FIME mDL Reader Test Case Specification
Test suite	FIME mDL Reader Test Suite v1.4.0
mDL Test App	mdlreadertestapp-1.4.0.apk
Test device on which the mDL Test App is installed	Samsung Galaxy S24
OS version of the test device on which the mDL Test App is installed	Android 14

Test Devices and Platform

Device brand and type	iPhone 15	iPhone SE (2nd Gen)
OS version	iOS 17.6.1	iOS 15.5

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

A.1 Implementation conformance statement

The Implementation Conformance Statements below were provided to FIME by Veridos and have been used to determine which test cases to execute.

The ICS version used by Veridos is v1.6.

A.1.1 General information

mDL owner	
Application owner Name	Veridos
Address	Oranienstraße 91, Berlin, Germany 10969
City	Berlin
State	Berlin
Zip Code / Postal Code	10969
Country	Germany
Contact Name	Nicholas Larter
Contact Title	Senior Solutions Manager
Contact Email Address	nick.larter@veridos.com
Contact Phone Number	+49 1525 1334198

#	mDL reader General Information	
-	Reader Application name and version	VD CheckID Version 1.0.6(6)
-	Minimum version of iOS supported	iOS 15



1.	Specify which DocType(s) the mDL reader supports	1
2.	For each DocType, specify which namespace(s) the mDL reader supports.	org.iso.18013.5.1.mDl
3.	For each namespace, specify the identifiers of all data elements that can be requested by the mDL reader.	family_name given_name birth_date document_number driving_privileges issue_date expiry_date issuing_authority issuing_country portrait un_distinguishing_sign sex height weight eye_colour hair_colour age_in_years age_birth_year birth_place nationality portrait_capture_date resident_address resident_city resident_state resident_postal_code resident_country signature_usual_mark family_name_national_character given_name_national_character age_over_18 age_over_19 age_over_20 age_over_21 age_over_22 age_over_23 age_over_24 age_over_25 age_over_26
4.	mDL reader is able to request multiple documents in a single DeviceRequest message.[1]	☐YES ☒NO
5.	mDL reader is able to request multiple documents in a single ServerRequest message.[2][3]	☐YES ☒NO

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo
.com

6.	mDL reader is able to request the issuing_jurisdiction data element from namespace org.iso.18013.5.1	☐YES ☒NO
7.	mDL reader is able to request the age_over_NN data element from namespace org.iso.18013.5.1	☒YES ☐NO
8.	mDL reader is able to request the issuing_country data element from namespace org.iso.18013.5.1	☒YES ☐NO

A.1.2 For technology test cases

#	ICS statements for Technologies Test cases	
9.	mdoc reader supports device engagement using NFC Static Handover. [1]	☒YES ☐NO
10.	mdoc reader supports device engagement using NFC Negotiated Handover. [2]	☒YES ☐NO
11.	mdoc reader supports device engagement using a QR code. [3]	☒YES ☐NO
12.	mdoc reader supports device retrieval using NFC. [4]	☒YES ☐NO
13.	mdoc reader supports device retrieval using BLE in mdoc central client mode. [5]	☒YES ☐NO
14.	mdoc reader supports device retrieval using BLE in mdoc peripheral server mode. [5]	☒YES ☐NO
15.	mdoc reader supports device retrieval using BLE version 5.0 (or above) and LE 2M PHY.	☐YES ☒NO
16.	mdoc reader supports device retrieval using Wi-Fi Aware.	☐YES ☒NO
17.	mdoc reader supports server retrieval using OIDC	☐YES ☒NO
18.	mdoc reader supports server retrieval using WebAPI.	☐YES ☒NO
19.	mdoc reader supports extended-length APDUs for device retrieval using NFC.	☒YES ☐NO
20.	mdoc reader supports the L2CAP transmission profile if it is acting as the GATT client for device retrieval using BLE.	☐YES ☒NO

[1] If this is set to YES, the mDL reader should support at least two different DocTypes.
[2] This statement is only applicable if the mDL reader supports server retrieval using WebAPI.
[3] If this statement is set to YES, the mDL reader should support at least two different DocTypes.
[4] Note this is mandatory to support for mDL readers, but optional for mdoc readers in general.



21.	mdoc reader supports the L2CAP transmission profile if it is acting as the GATT server for device retrieval using BLE.	☐YES ☒NO
22.	mdoc reader sends a ReaderEngagement structure as part of the Handover Request Message during device engagement using NFC Negotiated Handover.	☐YES ☒NO
23.	mdoc reader implements a time-out for the time between the transaction initialization and receiving device engagement data.	☐YES ☒NO
24.	If yes, indicate how long is the time-out (in seconds).	xx seconds
25.	mdoc reader implements a time-out for the time between receiving device engagement data and the successful set-up of a device retrieval connection.	☐YES ☒NO
26.	If yes, indicate how long is the time-out (in seconds).	xx seconds

A.1.3 For security mechanism test cases

#	ICS statements for Security Mechanisms test cases	
27.	mdoc reader supports mdoc reader authentication	☒YES ☐NO
28.	If yes, a test CRL for all mdoc reader authentication certificates used by the mdoc reader is available during testing.	☒YES ☐NO
29.	If yes, the CA that signed all mdoc reader authentication certificates used by the mdoc reader has an OCSP service.	☐YES ☒NO
30.	If yes, a test OCSP Responder for all mdoc reader authentication certificates used by the mdoc reader is available during testing.	☐YES ☒NO
31.	If yes, which curves does the mdoc reader use for mdoc reader authentication?	☒ Curve P-256 ☒ Curve P-384 ☒ Curve P-521 ☒ Ed25519 ☒ Ed448 ☒ brainpoolP256r1 ☒ brainpoolP320r1 ☒ brainpoolP384r1 ☒ brainpoolP512r1
32.	mdoc reader supports exchanging more than one device retrieval mdoc request and response with the mdoc in a single session.	☐YES ☒NO
33.	mdoc reader supports exchanging more than one server retrieval request and response with the issuing authority infrastructure in a single session.	☐YES ☒NO
34.	mdoc reader supports retrieving OCSP information, if available when verifying a TLS server certificate. [1]	☐YES ☒NO

[1] This statement is only applicable if the mdoc reader supports server retrieval using WebAPI.



35.	mdoc reader requests OCSP status information for the server certificate in the TLS handshake [1]	☐YES ☒NO
36.	mdoc reader supports TLS v 1.3. [1]	☐YES ☒NO
37.	mdoc reader supports TLS Client Authentication.	☐YES ☒NO
38.	If yes, a test CRL for all TLS Client certificates used by the mdoc reader is available during testing	☐YES ☒NO
39.	If yes to #34, the CA that signed all TLS Client authentication certificates used by the mdoc reader has an OCSP service.	☐YES ☒NO
40.	If yes, a test OCSP Responder for all TLS Client authentication certificate used by the mdoc reader is available during testing.	☐YES ☒NO
41.	How many seconds is the time-out period for session termination implemented by the mdoc reader?	300 seconds

780

I, notary representative, hereby certify that this document is a true copy of a pdf-file.

Munich, this 15.01.2025

Dr. Christian Linke,
notary representative of
Dr. Bernhard Schaub
Notary Public in Munich,
Federal Republic of Germany
(commission expires: October 31, 2032)

Die Echtheit vorstehender Unterschrift des Notarassessors Dr. Christian Linke und die Echtheit des beigedrückten Dienstsiegels werden hiermit bestätigt.
Zugleich wird bescheinigt, dass der Vorgenannte zur Vornahme der Amtshandlung befugt war.

München, 16. Januar 2025
Die Präsidentin des Landgerichts München I
Im Auftrag

Lea Adelsberger
Justizsekretärin

CONSORCIO EMDOC
EMDOC CONSORCIO
Santo Domingo, R.D.

781

Übersetzerin für die spanische Sprache
Susanne Bernhardt
Ravensburger Ring 18
81243 München

Übersetzer für die englische Sprache
Patrick Hampp
Nimitz-Kaserne-Allee 20
85540 Haar

EMBAJADA DE LA REPÚBLICA DOMINICANA
EN ALEMANIA
SECCIÓN CONSULAR

CERTIFICO, que la firma que aparece al pie de esta documentación, es la del/ de la Sr./a Adelsberger - Justicia Regional
CIUDAD Munchen **y que es** la misma que acostumbra a usar en todos sus actos y la cual es de su entera fé y crédito.
FECHA 12-02-2025

EMBAJADA DE LA REPÚBLICA DOMINICANA
SECCIÓN ALEMANIA

HEIDI TAVERAS
CONSEJERA

CONSORCIO EMDOC
EMDOC
Santo Domingo, R.D.

782

Certificación SIGMA

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo

xtek Mühlbauer GSI ULTRATECH VERIDOS

Ave. 27 de febrero esquina Ave. Tiradentes, Torre Piñana, Local 6-B
Santo Domingo, Rep. Dominicana, Tel. (809) 412-5312

783

Traducción certificada del alemán

COPIA CERTIFICADA

Safran+
Lean-Sigma

SAFRAN
University

CERTIFICADO

SAFRAN LEAN-SIGMA

Mike HAHN

ha cumplido con éxito los requisitos establecidos por Safran en cuanto

- a conocimientos en metodologías y herramientas de Lean & 6-sigma
- a la formación de Green Belt, Black Belt y de ejecutivos
- al entrenamiento de Green Belt & Black Belt
- a ayudando a ejecutivos a elaborar e implementar planes de mejora coherentes con los objetivos estratégicos y

POR LA PRESENTE SE CERTIFICA COMO

MASTER BLACK BELT LEAN-SIGMA

JUNIO de 2016

[*escrito a mano: Felicidades*]

Jean-Jacques ORSINI
Vicepresidente ejecutivo,
Rendimiento y Competitividad

[Firma]

SAFRAN

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

781

Yo, representante notarial, certifico que este documento es una copia fiel del documento original.

En Múnich, a 29/01/2025

[Sello del notario]

[Firma]

Dr. Bernhard Schaub
Notario en Múnich,
República Federal de Alemania
(el mandato expira el 31 de octubre de 2032)

Como traductora jurada y nombrada públicamente para los idiomas alemán, inglés y español en Baviera, confirmo que la traducción que precede del documento que se me ha presentado en lengua alemana es correcta y completa.

Múnich, a 6 de febrero del 2025

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

Öffentlich bestellte und beeidigte Übersetzerin für die spanische Sprache
Susanne Bernhardt
Ravensburger Ring 18
81243 München

9

785

Die Echtheit vorstehender Unterschrift der
Übersetzerin Susanne Bernhardt wird hiermit bestätigt.
Zugleich wird bescheinigt, dass die Vorgenannte
öffentlich bestellte und allgemein beeidigte
Übersetzerin für die spanische Sprache ist.

München, 12. Februar 2025
Die Präsidentin des Landgerichts München I
Im Auftrag

Lea Adelsberger
Justizsekretärin

EMBAJADA DE LA REPÚBLICA DOMINICANA
EN ALEMANIA
SECCIÓN CONSULAR

CERTIFICO, que la firma que aparece al pie de esta documentación es la del/ de la Sr/a. Adelsberger - Justizsekretärin
CIUDAD München **y que es la misma que acostumbra a usar en todos sus actos y la cual es de su entera fé y crédito.**
FECHA 14-02-2025

HEIDI TAVERAS
CONSEJERA

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

Beglaubigte Übersetzung aus dem Englischen

BEGLAUBIGTE KOPIE

Safran+
Lean-Sigma

SAFRAN
University

URKUNDE

SAFRAN LEAN-SIGMA

Mike HAHN

hat erfolgreich alle von Safran aufgestellten Anforderungen in Bezug auf

- das Expertenwissen im Bereich Lean- & 6-Sigma-Methoden & -Werkzeuge
- das Green-Belt-, Black-Belt- und Manager-Training
- das Green-Belt- & Black-Belt-Coaching
- Hilfestellung für Führungskräfte zu leisten bei der Ausarbeitung sowie der Umsetzung von Verbesserungsplänen im Einklang mit den strategischen Zielen

erfüllt und

WIRD HIERMIT ZERTIFIZIERT ALS

MASTER BLACK BELT LEAN-SIGMA

JUNI 2016

[handschriftlich: Glückwunsch] Jean-Jacques ORSINI [Unterschrift]
Executive VP,
Performance und Wettbewerbsfähigkeit

SAFRAN

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

Als Notar bestätige ich hiermit, dass dieses Dokument eine originalgetreue Abschrift des Originaldokuments ist.

München, den 29. Januar 2025

[Notarielles Siegel]

[Unterschrift]

Dr. Bernhard Schaub

Notar in München, Deutschland

(Kommission endet am 31. Oktober 2032)

Als in Bayern öffentlich bestellte und allgemein beeidigte Dolmetscherin für die englische Sprache bestätige ich: Vorstehende Übersetzung der mir im Original vorgelegten, in englischer Sprache abgefassten Urkunde ist richtig und vollständig.

München, den 06. Februar 2025

CONSORCIO EMDOC
EMDOC CONSORCIO
Santo Domingo, R.D.

Deutsche Beeidigte Dolmetscherin für die englische Sprache
Susanne Bernhard
Ramersdorfer Ring 18
81243 München

Certified Copy



789

I, Notary Public, hereby certify that this document is a true copy of the original document.

Munich, this 29.01.2025

Dr. Bernhard Schaub
Notary Public in Munich,
Federal Republic of Germany
(commission expires: October 31, 2032)

789-A

EMDOC
CONSORCIO

DETALLE DEL CRONOGRAMA CUMPLIMIENTO

PARA LA CONTRATACIÓN DE LA EMPRESA QUE SE ENCARGARÁ DE SUPLIR LOS EQUIPOS, MATERIALES Y SERVICIOS PARA LA IMPRESIÓN DE LA CÉDULA DE IDENTIDAD Y ELECTORAL (CIE) Y CÉDULA DE IDENTIDAD (CI)

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

789-D

EMDOC CONSORCIO

ETAPA 1: IMPLANTACIÓN Y PUESTA EN MARCHA DEL PROYECTO:

1.**Entregar el diseño de seguridad de las tarjetas** a las cuatro (4) semanas después de la firma de contrato. La JCE debe responder en una semana:
Actividad 16: Finalización del diseño gráfico y formato del documento
Cumple: Entrega de **4 semanas** a la JCE.

2. **Suministrar dos impresoras de policarbonato a las dieciséis** (16) semanas, así como 2,000 tarjetas genéricas de policarbonato con chip para pruebas.
Actividad 34: Entrega de 2 impresoras de personalización
Cumple: Entrega en **16 semanas** a la JCE.

3. **Instalar la PKI y la CA, así como realizar la ceremonia de llaves a las dieciséis (16) semanas.**
Instalar la PKI de Tarjeta Física y Digital
Actividad 227: Ceremonia de entrega de llaves realizada
Cumple: Entrega en **14 semanas.**

Instalar la PKI CA:
Actividad 226: Ceremonia de Llaves
Cumple: 15 semanas

4. **Ayudar a los técnicos de la JCE a adaptar el SDK** de la impresora al sistema de la JCE.
Actividad 36: Apoyo al técnico de JCE para adaptar las impresoras del SDK al sistema.
Cumple: Semana 6 a 9

5. **Realizar pruebas unitarias, de integración**, de pre-producción con las impresoras, las tarjetas, personalizando la tarjeta.
Actividad 39: Pruebas Unitarias de integración y aceptación SAT,
Cumple: Semana 9 a 10

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

6. Realizar las pruebas pilotо de la solución digital de la tarjeta CD (Mobile ID) antes de veintiséis (26) semanas, incluyendo el desarrollo de una app para la JCE.
Actividad 249: Pruebas
Cumple: Semana 20

7. Entrega de 300,000 tarjetas de policarbonato a las veintidós (22) semanas después de la firma de contrato. Esta entrega será acompañada con el reporte de laboratorio certificado e independiente, de los test de durabilidad de la tarjeta, así como el chip.
Actividad 249: Envío, importación y entrega de documentos genéricos (2000 unidades)
Cumple: Semana 13

789-€

8. **Capacitación al personal de la JCE** de la operación y mantenimiento del equipo deimpresión, PKI y solución digital.
Tarea 40:Capacitación Impresoras
Cumple: Semana 11

Etapa 2: Máximo 12 meses a partir del fin de la etapa 1. Re-cedulación total de la población (DEBE CUMPLIR CON TODO LO DESCRITO AQUI ABAJO)
el oferente adjudicado tendrá que realizar las siguientes actividades o entregar los siguientes elementos:

1. 500,000 tarjetas de policarbonato a las 26 semanas después de la firma de contrato.
   Cumple: Semana 26, tarea 25
2. 1,200,000 tarjetas de policarbonato a las 30 semanas después de la firma de contrato.
   Cumple: Semana 30, tarea 26
3. 1,000,000 tarjetas de policarbonato a las 34 semanas después de la firma de contrato.
   Cumple: Semana 34, tarea 27
4. 1,000,000 tarjetas de policarbonato a las 38 semanas después de la firma de contrato.
   Cumple: Semana 38, tarea 28
5. 1,000,000 tarjetas de policarbonato a las 42 semanas después de la firma de contrato.
   Cumple: Semana 42, tarea 29
6. 1,000,000 tarjetas de policarbonato a las 46 semanas después de la firma de contrato.
   Cumple: Semana 46, tarea 30
7. 1,000,000 tarjetas de policarbonato a las 50 semanas después de la firma de contrato.
   Cumple: Semana 50, tarea 31
8. 1,000,000 tarjetas de policarbonato a las 54 semanas después de la firma de contrato.
   Cumple: Semana 54, tarea 32
9. Adquisición e instalación de los equipos de impresión y puesta en marcha en las sedes de laRepública Dominicana y en el exterior. Las fechas de las entregas y cantidades de dichos equipos serán acordados con el proveedor adjudicado y la JCE.
   El Consorcio EMDOC entregará las siguientes impresoras de la siguiente manera:

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

789-D

- Entrega 2: 90 impresoras en Santo Domingo,tarea 46, semana 24, para distribuir en R. Dominicana.
- Entrega 3: 90 impresoras en Santo Domingo, tarea 60, semana 28 para distribuir en 72 en R. Dominicana y 18 que la JCE reembarcará para N. York.
- Entrega 4: 32 impresoras en Santo Domingo, tarea 89, semana 49 para reembarcar de la siguiente manera:
  - 11 N. York: 9 USA y 2 Canadá
  - 15 Madrid para distribuir en Madrid
  - El resto serán entregadas en R.Dominicana para distribuir según señale la JCE.

10. Puesta en marcha del mantenimiento de las impresoras en periodo de garantía. Para ello, el proveedor deberá de disponer de mínimo de dos (2) técnicos certificados en tecnología de impresión de tarjetas de identidad, y mínimo un total de diez (10) técnicos para soporte nacional de servicio para reparación de equipos en sitio durante el periodo de garantía. Para el exterior, el proveedor durante tiempo de garantía de las impresoras, deberá reparar en Nueva York (los equipos de Estados Unidos y Canadá) y en Madrid (los equipos de Europa), la JCE enviará las impresoras defectuosas a estos lugares según aplique.

    Cumple: La puesta en marcha de la garantía técnica sería: Inicio Periodo de Garantía Mantenimiento, línea 281. Semana 41. El Consorcio EMDOC cumple con las siguientes:

Nombre de tarea	Duración	Comienzo	Fin	Predecesoras	Nombres de recursos	% Completado
Implementación de la impresora (90 impresoras)	150 días	vie. 09/05/25 9:00	jue. 04/12/25 19:00		Consorcio EMDOC	0%
Fase de comprobación previa de las ubicaciones de las impresoras (estudio del emplazamiento)	10 días	vie. 09/05/25 9:00	jue. 22/05/25 19:00			0%
Verificación del espacio físico, las mesas y las conexiones eléctricas y de datos.	1 sem	vie. 09/05/25 9:00	jue. 15/05/25 19:00	11	Consorcio EMDOC	0%
Documento de informe de estado de los requisitos.	1 sem	vie. 16/05/25 9:00	jue. 22/05/25 19:00	49	Consorcio EMDOC	0%

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

789-E

EMDOC
CONSORCIO

11. ACLARACION IMPORTANTE El sistema de cedulación actual permanece igual. No está incluido en el alcance de esta licitación. Los componentes del concurso deben integrarse a los sistemas actuales, proporcionando el oferente todos los SDK necesarios, los APIS de integración y apoyando en su caso a la Dirección de Informática en su instalación y puesta en marcha. NOTA: La JCE podrá acordar con el adjudicatario el cambio de fechas o de cantidad, por problemas de almacenamiento o de consumo de las tarjetas.

Etapa 3: 12 meses renovable a 10 años. El mantenimiento en todos los casos es solamente por 2 años.

- Suministrar tarjetas en la oficina Central de la JCE en base a la demanda que se requiera durante la vigencia del contrato que se estima en 1,000,000 de tarjetas al año, siempre un 10% CI. En todo momento la responsabilidad de poseer disponibilidad de CIs y CIEs es del proveedor.

  Serán acordados con la JCE y podrán ser suministrados una vez se cumpla el período y se cumplirá con las entregas planificadas.

- 2. Proveer mantenimiento de los equipos de impresión mientras los equipos estén en garantía. Cuando termine la garantía, los equipos deberán ser atendidos en las siguientes localidades:
- Para los centros de cedulación ubicados en todo el territorio nacional, serán atendidos en la sede central de la JCE. Para las oficinas OSE ubicadas en Estados Unidos de Norte América, serán atendidas en la OSE de New York.
- Para las oficinas OSE ubicadas en Europa, serán atendidas en la OSE de Madrid.
- Para las demás oficinas ubicadas en otras demarcaciones, serán atendidas en la Sede

El Consorcio EMDOC cumple con las siguientes:

  - Tarea 283, Mantenimiento Impresoras R. Dominicana, después de 8 meses de entregada la última impresora.
  - Tarea 284, Mantenimiento Impresora USA (N.York), después de 6 meses de finalizada la última entrega.
  - Tarea 285, Mantimiento Impresoras Europa (Madrid), después de 6 meses de finalizada la última entrega.
- Central de la JCE.
  - Tarea 283, Mantenimiento Impresoras R. Dominicana, después de 8 meses de entregada la última impresora. Iniciando con Central de la JCE

- 3. Proveer mantenimiento de nivel 3 para el mantenimiento del sistema y equipos PKI, y sistemas y equipos para la tarjeta digital.
- **Se realizarán 4 mantenimientos** desglosados de la siguiente manera:

789-F

EMDOC CONSORCIO

Nombre de tarea	Duración	Comienzo	Fin
Etapa 3: Operación y Mantenimiento	**730 días**	**lun 8/12/25**	**vie 22/9/28**
Primer Período de Mantenimiento Año 1	**365 días**	**lun 8/12/25**	**vie 30/4/27**
Mantenimiento de las Impresoras y Capacitación R. Dominicana	16 sem.	lun 17/8/26	vie 4/12/26
Mantenimiento de las Impresoras y Capacitación USA (N.York)	7 sem.	lun 7/12/26	vie 22/1/27
Mantenimiento de las Impresoras y Capacitación Europa (Madrid)	7,1 sem.	lun 25/1/27	lun 15/3/27
Mantenimiento de las Impresas y Capacitación R. Mundo	2 sem.	lun 15/3/27	lun 29/3/27
Mantenimiento Centro de Datos 1 y Capacitación (inc. PKI, Mobile ID; PKICA y HW)	27 días	lun 8/12/25	mar 13/1/26
Mantenimiento 2: Centro de Datos 1 (inc. PKI, Mobile ID; PKICA y HW)	27 días	lun 25/5/26	mar 30/6/26
Cierre de Primer Año 1	34,5 días	lun 15/3/27	vie 30/4/27
Segundo Período de Mantenimiento Año 2	**365 días**	**lun 3/5/27**	**vie 22/9/28**
Mantemiento Impresoras R. Dominicana	16 sem.	lun 3/5/27	vie 20/8/27
Mantenimiento Impresora USA (N.York)	7 sem.	lun 23/8/27	vie 8/10/27
Mantimiento Impresoras Europa (Madrid)	7 sem.	lun 11/10/27	vie 26/11/27
Mantenimiento Impresoras R. Mundo	2 sem.	lun 29/11/27	vie 10/12/27
Mantenimiento Centro de Datos 1 (inc. PKI, Mobile ID; PKICA y HW)	35 días	lun 13/12/27	vie 28/1/28
Mantenimiento 2: Centro de Datos 1 (inc. PKI, Mobile ID; PKICA y HW)	35 días	lun 17/7/28	vie 1/9/28
Cierre de Proyecto	15 días	lun 4/9/28	vie 22/9/28

CONSORCIO EMDOC EMDOC CONSORCIO SANTO DOMINGO, R.D.

3.1.6.2 Requisitos de experiencia (Obligatorios)



790

Requisitos de experiencia (Obligatorios)

CONSORCIO EMDOC, Santo Domingo, R.D.

Experiencia en suministro de impresoras de documentos de identidad de policarbonato electrónicos

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

MINISTERIO DE GOBERNACIÓN Y POLICÍA / DIRECCIÓN GENERAL DE MIGRACIÓN Y EXTRANJERÍA | GOBIERNO DE COSTA RICA

792

San José, Costa Rica, 22 de mayo de 2024.GM
Gm-0110.06-2024

Señores
Junta Central Electoral (JCE)
República de Dominicana
Su Oficina

Ref: JCE-CCC-LPI-2024-0001 «Contratación de la empresa que se encargará de suplir los equipos, materiales y servicios para la impresión de la nueva Cédula de Identidad y Electoral (CIE) y Cédula de Identidad (CI)».

Estimados señores:

Después de expresarle un cordial saludo, muy respetuosamente me permito informarle.

"Que mediante el Fideicomiso Fondo Especial de Migración JADGME – BCR, se tramitó el proceso de licitación pública 2019PP-000068-0016200001 Pasaporte Biométrico, para adquirir un sistema de emisión de documentos migratorios, para la Dirección General de Migración y Extranjería de Costa Rica, entre ellos, pasaportes biométricos de policarbonato, la compra de equipos tecnológicos, libretas de pasaportes biométricos de policarbonato, soporte y mantenimiento de la solución a través de la empresa GSI-Veridos, el monto de contratación asciende a más de $9 millones de USD a la fecha".

Esta contratación incluyó la adquisición de impresoras de pasaportes biométricos de policarbonato, además incluyó la instalación de este equipo, pruebas y puesta en producción, integración del sistema, así como, el mantenimiento de la solución de personalización.

En la ejecución del contrato antes señalado, es importante indicar que, la empresa GSI-Veridos ha cumplido con el contrato a satisfacción.

Cordialmente se despide de ustedes muy atentamente.

Rosibel Vargas Durán
Gestora
Gestión de Migraciones
Dirección General de Migración y Extranjería
rvargasd@migracion.go.cr

GESTIÓN MIGRACIONES

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

c.c. Archivo.

793

MINISTERIO DE GOBERNACIÓN Y POLICÍA / DIRECCIÓN GENERAL DE MIGRACIÓN Y EXTRANJERÍA | GOBIERNO DE COSTA RICA

REPÚBLICA DE COSTA RICA

MINISTERIO DE RELACIONES EXTERIORES Y CULTO

A-111106208

APOSTILLE

(Convention de La Haye du 5 octobre 1961)

1. País: Costa Rica
(Country – Pays:)

Código: RGD3K7JOX59
(Code – Code:)

El presente documento público
(This public document – Le présent acte public)

2. Ha sido firmado por: Rosibel Vargas Duran
(Has been signed by – A été signé par:)

3. Actuando en calidad de: Gestor (a) de Migraciones
(Acting in the capacity of – Agissant en qualité de:)

4. Lleva el sello/estampilla de: Dirección General de Migración y Extranjería
(Bears the seal/stamp of – Est revêtu du sceau/timbre de:)

Certificado
(Certified – Attesté)

5. En: San José, Costa Rica
(At – A:)

6. El: 06/06/2024
(On – Le:)

7. Por: Ivannia Espinoza Rodriguez , Oficial de Autenticaciones
(By – Par:) Ministry of Foreign Affairs – Ministère des Affaires Etrangères

8. No.: 1101281
(Under number – Sous le numéro:)

9. Sello:
(Seal – Sceau:)

10. Firma:
(Signature – Signature:)

1106208

Este apostilla / legalización sólo certifica la autenticidad de la firma, la capacidad del signatario y el sello o timbre que ostenta. Esta no certifica el contenido del documento para el cual se expidió.

This apostille / legalization only certifies the signature, the capacity of the signer and the seal or stamp it bears. It does not certify the content of the document for which it was issued.

Cette apostille / legalization ne certifie que la signature, la qualité en laquelle le signataire de l'acte a agi, et le sceau ou timbre dont cet acte est revêtu. Elle ne certifie pas le contenu du document pour lequel elle a été émise.

La autenticidad de esta apostilla / legalización puede ser verificada en: - The authenticity of this apostille / legalization may be verified at: - L'authenticité de cette apostille / legalization peut être vérifiée sur: http://www.rree.go.cr

CONSORCIO EMDOC CONSORCIO EMDOC Santo Domingo, R.D.

Beglaubigte Ablichtung
794

Montenegro
Ministry of Interior

Bulevar Svetog Petra Cetinjskog br.22,
81000 Podgorica, Crna Gora
Tel/fax: +382 20 246 917
www.mup.gov.me

Service for information technologies

No: 41-900/24-3191 Podgorica, 6.6.24 year

Contact Details: Dejan Žarkovic
Chief of the Bureau for public key infrastructure and personalization documents
+382 67 286 676
dejan.zarkovic@mup.gov.me

To who it may concern:

JUNTA CENTRAL ELECTORAL

Comisión de Compras y Contrataciones

Referencia: JCE-CCC-LPI-2024-0001

Gregorio Luperón Ave. esq. 27 de febrero Ave.,

Edificio administrativo, ala este, 2do nivel.

Confirmation of Expertise in	Confirmación de experiencia en
• Supply of electronic polycarbonate ID card printers • Supply of electronic polycarbonate ID Cards • Systems integration in electronic identification project	• Suministro de impresoras de tarjetas de identificación electrónicas en policarbonato • Suministro de tarjetas de identificación electrónicas en policarbonato • Integración de sistemas en el proyecto de identificación electrónica
We hereby confirm that the company Mühlbauer ID Services GmbH has been entrusted with the implementation of an Identity Document Issuing System under contract number 404/19/308583/1. The scope of work includes: - The design and supply of ID cards based on polycarbonate material with dual interface (contact and contactless) chip component for the project	Por la presente confirmamos que se ha adjudicado a la empresa Mühlbauer ID Services GmbH la realización de un sistema de emisión de documentos de identificación con el número de contrato 404/19/308583/1. El alcance del trabajo incluye: - El diseño y suministro de tarjetas de identificación en policarbonato con componente de chip de doble interfaz (con y sin contacto) para el proyecto

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

- The design and supply of driving license cards based on polycarbonate material without chip component for the project	- El diseño y suministro de tarjetas de permiso de conducir en policarbonato sin componente chip para el proyecto
- The design and supply of ePassports with a polycarbonate data page for the project	- El diseño y suministro de pasaportes electrónicos con una página de datos en policarbonato para el proyecto
- The provision of personalization machines and a personalization management system	- El suministro de máquinas de personalización y un sistema de gestión de la personalización
o Card Personalization Machines Mühlbauer SCP 501	o Máquinas de personalización de tarjetas Mühlbauer SCP 501
o Passport Personalization Machines Mühlbauer Identifier 60	o Máquinas de personalización de pasaportes Mühlbauer Identifier 60
o Personalization Management System MB INCAPE	o Sistema de gestión de la personalización MB INCAPE
- Integration and implementation of the systems in an existing technology infrastructure	- Integración e implementación de los sistemas en una infraestructura tecnológica existente
- Maintenance and support for the systems (Personalization Management System, Server Systems, Card Personalization Machines, Passport Personalization Machines).	- Mantenimiento y soporte de los sistemas (Sistema de Gestión de Personalización, Sistemas Servidores, Máquinas de Personalización de Tarjetas, Máquinas de Personalización de Pasaportes).
The installed technology provided is operated by the authorities' personnel. Maintenance and servicing is carried out by Mühlbauer.	La tecnología instalada proporcionada es operada por el personal de las autoridades. El mantenimiento y el servicio son llevados a cabo por Mühlbauer.
The concluded contract is in active status, was concluded on July 30, 2019 and is valid for 42 months.	El contrato suscrito se encuentra en estado activo, se concertó el 30 de julio de 2019 y es válido por 42 meses.
With pleasure, we herewith confirm the successful cooperation with Mühlbauer ID Services GmbH who supported us in all matters in a flexible and client orientated manner and we additionally confirm that the company fulfilled all our expectations.	Nos complace confirmar por la presente la exitosa cooperación con Mühlbauer ID Services GmbH, que nos ha brindado soporte en todas las cuestiones de forma flexible y orientada al cliente, y confirmamos además que la empresa ha cumplido todas nuestras expectativas.

Yours sincerely,

CONSORCIO EMDOC Santo Domingo, R.D.

HEAD OF SERVICE
Daro Bečanović

796

Die Ablichtung stimmt mit der Urschrift überein.
Roding, 19. JUNI 2024
Marchner
Notarin

Gz. 91 E 205/2024

Die Echtheit vorstehender Unterschrift von

Notarin Katharina Marchner in Roding

und die Echtheit des beigedrückten Dienstsiegels werden hiermit bestätigt.

Zugleich wird bescheinigt, dass der/die Vorgenannte zur Vornahme der Amtshandlung gesetzlich befugt war.

Regensburg, den 19. Juni 2024
Der Präsident des Landgerichts
Im Auftrag

Manuela Wanner

Manuela Wanner
Justizangestellte

BAYERN LANDGERICHT REGENSBURG

Kostenrechnung
Gebühr: 25,00 €
(gem. Art. 1 Abs. 1 LJKostG, i.V.m. § 4 Abs. 1 JVKostG, KV 13.10

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo

797

Untermain 2, 60313 Frankfurt am Main, Alemania,
Tel. 49 69 74 38 77 81 / Fax: 49 69 74 38 76 43
www.consuladodominicanofrkf@hotmail.com

Consulado General
de la República Dominicana
en Frankfurt, Alemania

Reg.00283/2024

CONSULADO GENERAL DE LA REPUBLICA DOMINICANA EN FRANKFURT, ALEMANIA.

CERTIFICO Y DOY FE (sin entrar en el contenido del documento ni ulterior destino que pueda dársele): que la firma que aparece al pie de **ESTA COPIA NOTARIAL**, Identificado con el **No. S/N**, de fecha **19 DE JUNIO DEL 2024,** corresponde **A LA SRA. MANUELA WANNER, PRESIDENTE DE LA AUDIENCIA PROVINCIAL**, de la ciudad de REGENSBURG, Alemania.

Y que es la Firma que acostumbra a usar en todos sus actos y a la cual se debe entera fe y crédito.

En Frankfurt am Main, Alemania, a los veintiún (21) dias del mes de junio del año dos mil veinticuatro (2024).

Niovel Aurora Tapia Ortiz
Vicecónsul

CONSULADO GENERAL DE LA REPUBLICA DOMINICANA · FRANKFURT, ALEMANIA ·

CONSORCIO EMDOC
EMDOC CONSULADO
Santo Domingo, R.D.

798





XL/

799

JOSÉ MIGUEL GUERRA GONZÁLEZ
Intérprete Judicial

Yo, José Miguel Guerra González, Intérprete Judicial del Juzgado de Primera Instancia del Distrito Nacional, República Dominicana, debidamente juramentado para el ejercicio de mis funciones, CERTIFICO: Que he traducido un documento escrito en inglés, español y alemán cuya versión en español, a mi mejor entender, es la siguiente:

Copia Certificada

Montenegro
Ministerio del Interior

Bulevar Svetog Petra Cetinjskog br.22,
81000 Podgorica, Crna Gora
Tel/fax: +382 20 246 917
www.mup.gov.me

Servicio de Tecnologías de la Información

No. 48-900/24-31901

Podgorica, 6/6/24

Detalles de Contacto: Dejan Zarkovic
Encargado de la Oficina de Infraestructura de Llave Pública y Personalización de Documentos
+382 67 286 676
dejan.zarkovic@mup.gov.me

A Quien Pueda Interesar:
JUNTA CENTRAL ELECTORAL
Comisión de Compras y Contrataciones
Referencia: JCE-CCC-LPI-2024-0001
Ave. Gregorio Luperón esq. Ave. 27 de febrero,
Edificio administrativo, ala este, 2do nivel

Confirmación de experiencia en

- Suministro de impresoras de tarjetas de identificación electrónicas en policarbonato
- Suministro de tarjetas de identificación electrónicas en policarbonato
- Integración de sistemas en el proyecto de identificación electrónica

Por la presente confirmamos que se ha adjudicado a la empresa Mühlbauer ID Services GmbH la realización de un sistema de emisión de documentos de identificación con el número de contrato 404/19/[illegible]. El alcance del trabajo incluye:

- El diseño y suministro de tarjetas de identificación en policarbonato con componente de chip dual/doble interfaz (con y sin contacto) para el proyecto

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

800

- El diseño y suministro de tarjetas de permiso de conducir en policarbonato sin componente chip para el proyecto
- El diseño y suministro de pasaportes electrónicos con una página de datos en policarbonato para el proyecto
- El suministro de máquinas de personalización y un sistema de gestión de la personalización
- Máquinas de personalización de tarjetas Mühlbauer SCP 501
- Máquinas de personalización de pasaportes Mühlbauer Identifier 60
- Sistema de gestión de la personalización MB INCAPE
- Integración e implementación de los sistemas en una infraestructura tecnológica existente
- Mantenimiento y soporte de los sistemas (Sistema de Gestión de Personalización, Sistemas Servidores, Máquinas de Personalización de Tarjetas, Máquinas de Personalización de Pasaportes).

La tecnología instalada proporcionada es operada por el personal de las autoridades. El mantenimiento y el servicio son llevados a cabo por Mühlbauer.

El contrato suscrito se encuentra en estado activo, se concertó el 30 de julio de 2019 y es válido por 42 meses.

Nos complace confirmar por la presente la exitosa cooperación con Mühlbauer ID Services GmbH, que nos ha brindado soporte en todas las cuestiones de forma flexible y orientada al cliente, y confirmamos además que la empresa ha cumplido todas nuestras expectativas.

Atentamente,

Jefe del Servicio
Daro Becanovic

[Firmado]

[Sello: *Ilegible* - Podgorica]

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo

801

La copia anterior corresponde al documento original.

Roding, 19 de junio de 2024

[Firmado]
Notaria
[Sello: Katharina Marchner, Notaria de Roding]

No. de archivo 91 E 205/2024

Por este medio certifico la autenticidad de la firma que precede de la **Notaria Katharina Marchner de Roding,**

así como la autenticidad del sello oficial añadido.

Además, certifico que la persona antes mencionada está legalmente autorizada a ejecutar este acto oficial.

Ratisbona, el 19 de junio de 2024
La Presidenta del Tribunal Regional
De orden

[Firmado]
Manuela Wanner
Oficial Judicial

[Sello: Tribunal Regional de Ratisbona, Baviera]

Desglose de Costos
Impuesto: 25.00 €
(según el Art. 1, Párrafo 1 de la Ley de Costos Judiciales Estatales (LJKostG), en conjunto con la Sección 4, Párrafo 1 de la Ley de Costos de la Administración Judicial (JVKostG), KV 13.10)

El documento que antecede fue traducido en Santo Domingo, capital de la República Dominicana, el día 26 de julio del año 2024, y está registrado en mis archivos como "Carta de Referencia (Montenegro) MUHLBAUER ID SERVICES GMBH 2024072601".

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

Lic. José Miguel Guerra González
INTÉRPRETE JUDICIAL DEL JUZGADO DE PRIMERA INSTANCIA
República Dominicana

JOSÉ MIGUEL GUERRA GONZÁLEZ
Intérprete Judicial
Tralega Traducciones Legales, Intérpretes Judiciales
809-535-3011 / 809-535-6011 tralega.com info@tralega.com

802

República Dominicana
MINISTERIO DE RELACIONES EXTERIORES
Viceministerio para Asuntos Consulares y Migratorios
Dirección de Legalización de Documentos

APOSTILLA

(Convention de la Haye du 5 octobre 1961)

1.País:
Country / Pays: REPÚBLICA DOMINICANA

El presente documento público
This public document / Le présent acte public

2.Ha sido firmado por:
Has been signed by / A été signé par: NIOVEL AURORA TAPIA ORTIZ

3.Quien actúa en calidad de:
Acting in the capacity of / Agissant en qualité de: VICECÓNSUL

4.Y esté revestido del sello / timbre de:
Bears the seal / stamp of
Est revêtu du sceau / timbre de: CONSULADO GENERAL DE LA REPUBLICA DOMINICANA EN FRANKFURT, REPUBLICA FEDERAL DE ALEMANIA

Certificado
Certified / Attesté

5.En: Al / À	SANTO DOMINGO	**6.El día:** The / Le	29/7/2024
7.Por: By / Par	OPINIO ANTONIO DIAZ VARGAS - VICEMINISTRO ASUNTOS CONSULARES Y MIGRATORIOS	**8.Bajo el número:** N° / Sous°	AP-2024-7-29-703
9.Sello / Timbre: Seal / Stamp Sceau / Timbre		**10.Firma:** Signature	

Verificación
Verification / Vérification

País Destino:	REPÚBLICA DOMINICANA	**Código de verificación:**	YGYH53JBMGNG82L

Esta Apostilla certifica únicamente la autenticidad de la firma, la calidad en que el signatario del documento haya actuado, y en su caso, la identidad del sello o timbre del que el documento público está revestido.

This Apostille only certifies the authenticity of the signature and the capacity of the person who has signed the public document, and, where appropriate, the identity of the seal or stamp which the public document bears.

Cette Apostille atteste uniquement la véracité de la signature, la qualité en laquelle le signataire de l'acte a agi et, le cas échéant, l'identité du sceau ou timbre dont cet acte public est revêtu.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

803

Experiencia en proyecto de suministro de tarjetas de identidad electrónicas de policarbonato

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

MINISTERIO DE GOBERNACIÓN Y POLICÍA / DIRECCIÓN GENERAL DE MIGRACIÓN Y EXTRANJERÍA | GOBIERNO DE COSTA RICA

804

San José, Costa Rica, 22 de mayo de 2024.
GM-109-06-2024

Señores
Junta Central Electoral (JCE)
República de Dominicana
Su Oficina.

Ref: JCE-CCC-LPI-2024-0001 «Contratación de la empresa que se encargará de suplir los equipos, materiales y servicios para la impresión de la nueva Cédula de Identidad y Electoral (CIE) y Cédula de Identidad (CI)».

Estimados señores:

Después de expresarles un cordial saludo, muy respetuosamente me permito informales.

"Que mediante el Fidelcomiso Fondo Especial de Migración JADGME – BCR , se tramitó el proceso de licitación pública Número 2019PP-000068-0016200001 Pasaporte Biométrico, para adquirir un sistema de emisión de documentos migratorios, que expide la Dirección General de Migración y Extranjería de Costa Rica, entre ellos pasaporte biométrico de policarbonato, la compra de equipos tecnológicos y suministro de más de 1.000,000 de **libretas de pasaporte electrónicas de policarbonato, además de** soporte y mantenimiento a la solución; el cual lo realiza la empresa GSI-Veridos, el monto de contrato asciende a más de $9 millones de USD a la fecha".

En la ejecución del contrato citado anteriormente, es importante indicar, que la empresa GSI-Veridos ha cumplido con el contrato a satisfacción.

Cordialmente se despide de ustedes muy atentamente.

Rosibel Vargas Durán
Gestora
Gestión de Migraciones
Dirección General de Migración y Extranjería
rvargasd@migracion.go.cr

GESTIÓN MIGRACIONES

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

C.C Archivo

805

REPÚBLICA DE COSTA RICA

MINISTERIO DE RELACIONES EXTERIORES Y CULTO

A-11 06 2024

APOSTILLE

(Convention de La Haye du 5 octobre 1961)

1. País: Costa Rica
(Country – Pays:)

Código: RGD0UCBEAQ7
(Code – Code:)

El presente documento público
(This public document – Le présent acte public)

2. Ha sido firmado por: Rosibel Vargas Duran
(Has been signed by – A été signé par:)

3. Actuando en calidad de: Gestor (a) de Migraciones
(Acting in the capacity of – Agissant en qualité de:)

4. Lleva el sello/estampilla de: Dirección General de Migración y Extranjería
(Bears the seal/stamp of – Est revêtu du sceau/timbre de:)

Certificado
(Certified – Attesté)

5. En: San José, Costa Rica
(At – A)

6. El: 06/06/2024
(On – Le:)

7. Por: Ivannia Espinoza Rodriguez , Oficial de Autenticaciones
(By – Par:) Ministry of Foreign Affairs – Ministère des Affaires Étrangères

8. No.: 1101282
(Under number – Sous le numéro:)

9. Sello:
(Seal – Sceau:)

10. Firma:
(Signature – Signature:)

1106209

Esta apostilla / legalización sólo certifica la autenticidad de la firma, la capacidad del signatario y el sello o timbre que ostenta. Ésta no certifica el contenido del documento para el cual se expidió.

This apostille / legalization only certifies the signature, the capacity of the signer and the seal or stamp it bears. It does not certify the content of the document for which it was issued.

Cette apostille / legalization ne certifie que la signature, la qualité en laquelle le signataire de l'acte a agi, et le sceau ou timbre dont cet acte est revêtu. Elle ne certifie pas le contenu du document pour lequel elle a été émise.

La autenticidad de esta apostilla / legalización puede ser verificada en: - The authenticity of this apostille / legalization may be verified at: - L'authenticité de cette apostille / legalization peut être vérifiée sur: http://www.rree.go.cr

Descuento: 37.50
Total Timbres: 587.50

NICOLE SOLIS ROMERO
CAJERA

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D

306

1 Hojas de 2

REGISTRO NACIONAL DE LAS PERSONAS
GUATEMALA, C.A.

Guatemala, 30 de mayo de 2024

JUNTA CENTRAL ELECTORAL
Comisión de Compras y Contrataciones
Referencia: JCE-CCC-LPI-2024-0001
Gregorio Luperón Ave. esq. 27 de febrero Ave.,
Edificio administrativo, ala este, 2do nivel.

Confirmación de experiencia en suministro de documentos de identidad en policarbonato con chip.

Mühlbauer ID Services GmbH, como contratista principal del "Registro Nacional de las Personas" (RENAP) de Guatemala, entregó en calidad de fabricante 6.000.000 Documentos Personales de Identidad entre 2019 y 2024 para la emisión del programa del Documento Nacional de Identidad, denominado "DOCUMENTO PERSONAL DE IDENTIFICACIÓN " (DPI).

Por la presente, confirmamos que Mühlbauer ID Services GmbH entregó documentos de identificación electrónicos 100% de policarbonato de acuerdo con las normas internacionales, tales como ANSI / NIST, ANSI/INCITS, ISO/IEC, FIPS 140-2 Nivel 3, Criterios Comunes EAL5 y OACI Doc. 9303.

Las tarjetas DPI están equipadas con un chip basado en contacto. En el chip se almacenan diferentes aplicaciones, incluida una aplicación Match-on-Card para una verificación cómoda y eficaz de las huellas dactilares, así como un applet de identificación y viaje de la OACI.

Además, confirmamos el suministro correcto y conforme de los DPI **(Documento Nacional de Identidad en policarbonato con chip)** en el periodo correspondiente:

Contrato	Duración del contrato	Volumen de documentos contratados en unidades	Importe contratado incl. 12% IVA / VAT en GTQ
Contrato no. 1	10/2019 - 10/2020	2,000,000	25,120,000.- GTQ
Contrato no. 2	06/2020 - 11/2021	2,000,000	24,520,000.- GTQ
Contrato no. 3	07/2022 - 09/2023	2,000,000	27,000,000.- GTQ

Nos complace confirmar por la presente la exitosa colaboración con Mühlbauer ID Services GmbH, que nos ha proporcionado soporte en todas las cuestiones de forma flexible y orientada al cliente, y confirmamos además que Mühlbauer ID Services GmbH ha cumplido todas nuestras expectativas en cuanto a precio y fecha de entrega, tal y como se acordó en el contrato.

Cordial saludo,

Dr. Rodolfo Estuardo Arriaga Herrera
Director Ejecutivo
Registro Nacional de las Personas -RENAP-
Guatemala, Guatemala
Número de teléfono: +50 224 1619 00
Correo electrónico: rarriaga@renap.gob.gt

Licenciada
Ruth Mercedes Hernández Mendoza
Abogada y Notaria

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

807

2 Hojas de 2

En la ciudad de Guatemala, departamento de Guatemala, el día treinta de mayo de dos mil veinticuatro, **COMO NOTARIA DOY FE**, que la anterior hoja de fotocopia, impresa en su lado anverso únicamente es **AUTENTICA** por haber sido reproducida fielmente de su original el dia de hoy en mi presencia, y que la misma reproduce **CARTA DE CONFIRMACION DE EXPERIENCIA** emitida por el Director ejecutivo del Registro Nacional de las Personas -RENAP- de la República de Guatemala, razón por la cual, numero, sello y firmo la anterior hoja de fotocopia y la presente.

POR MI Y ANTE MI:

Licenciada
Ruth Mercedes Hernández Mendoza
Abogada y Notaria



CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

808

GUATEMALA, C.A.

ORGANISMO JUDICIAL DE LA REPÚBLICA DE GUATEMALA
ARCHIVO GENERAL DE PROTOCOLOS
REGISTRO ELECTRÓNICO DE NOTARIOS
GUATEMALA, C.A.

2024-8964/ASANCHEZ

LA INFRASCRITA SUBDIRECTORA DEL ARCHIVO GENERAL DE PROTOCOLOS DEL ORGANISMO JUDICIAL DE LA REPÚBLICA DE GUATEMALA, CERTIFICA: Que la firma de el (la) Notario (a) **RUTH MERCEDES HERNANDEZ MENDOZA** es AUTÉNTICA, en virtud de ser la que corresponde a el (la) citado (a) notario (a) de conformidad con el Registro veinte mil ochocientos noventa de Folio trece mil novecientos setenta y cuatro del Libro seis-E del Registro Electrónico de Notarios que obra en este Archivo.

La suscrita, no prejuzga ni asume responsabilidad alguna por el contenido ni por la eficacia jurídica del documento, de cuya firma se legaliza.

TARIFA: Q. 150.00 ACUERDO 24-2011 DE LA CORTE SUPREMA DE JUSTICIA. Formulario Electrónico de Ingresos -FEI- 122381061927.

Guatemala, tres de junio de dos mil veinticuatro.

Licda. Lidia Judith Urizar Castellanos
Coordinador II
Subdirector Metropolitano
Archivo General de Protocolos

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

809

República de Guatemala

MINISTERIO DE RELACIONES EXTERIORES

APOSTILLE

(Convention de La Haye du 5 octobre 1961)

Código de Verificación: 82KsMv

VERIFICACIÓN EN LINEA:

https://minex.gob-gt.my.site.com/

Digitally signed by MINISTERIO DE RELACIONES EXTERIORES
Date: 07/06/2024
Reason: LEGALIZACION DE COPIA DE DOCUMENTO
Location: https://minex.gob-gt.my.site.com/
La presente apostilla no surte efecto en Guatemala

1. **País: República de Guatemala**
(country / Pays:)

El presente documento público
(this public document / le présent acte public)

2. **Ha sido firmado por:** LIDIA JUDITH URIZAR CASTELLANOS
(has been signed by / a été signé par:)

3. **Quien actúa en la calidad de:** COORDINADOR II SUBDIRECTOR METROPOLITANO
(acting in capacity of / agissant en qualité de:)

4. **Y está revestido del sello / timbre de:** ARCHIVO GENERAL DE PROTOCOLOS
(Bears the seal / stamp of / est revêtu du sceau / timbre de:)

Certificado
Certificate / Attesté

5. **En:** GUATEMALA
(at / à:)

6. **El día:** 07/06/2024
(the / le:)

7. **Por:** JOSE DAVID DE LA CRUZ FIGUEROA
(by / par:)

8. **Bajo el número:** 00000217822024
(number / sous n°:)

MINISTERIO DE RELACIONES EXTERIORES
DEPARTAMENTO DE AUTENTICAS
GUATEMALA, C.A.

9. **Sello / timbre**
(seal/stamp – sceau/timbre:)

Impuesto del Timbre Fiscal pagado según Decreto 37-92 del Congreso de la República de Guatemala con Formulario SAT 7130 No. 428963842S3

10. **Firma**
(signature / signature:)

El Ministerio de Relaciones Exteriores no asume responsabilidad alguna por el contenido ni por la eficacia jurídica de este documento y la presente legalización se limita a reconocer la autenticidad de la firma del funcionario en referencia.

The Ministry of Foreign Affairs does not assume any responsibility for the contents or validity of this document and merely authenticates the signature of the officer involved.

Le Ministère des Affaires Étrangères n'est pas responsable, en aucun cas, du contenu ni de l'efficacité juridique de ce document et la présente légalisation se limite à reconnaître l'authenticité de la signature du fonctionnaire en référence.

CONSORCIO EMDOC
EMDOC CONSORCIO
Santo Domingo, R.D.

Experiencia en un proyecto de suministro de tarjetas de identidad electrónicas de policarbonato de transición de documentos de identificación mecánicos (sin electrónica) a documento de identificación electrónicos

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

MINISTERIO DE GOBERNACIÓN Y POLICÍA / DIRECCIÓN GENERAL DE MIGRACIÓN Y EXTRANJERÍA | GOBIERNO DE COSTA RICA

811

San José, Costa Rica, 22 de mayo de 2024.
GM-0111-06.2024

Señores
Junta Central Electoral (JCE)
República de Dominicana
Su Oficina.

Ref: JCE-CCC-LPI-2024-0001 «Contratación de la empresa que se encargará de suplir los equipos, materiales y servicios para la impresión de la nueva Cédula de Identidad y Electoral (CIE) y Cédula de Identidad (CI)».

Estimados señores:

Después de expresarles un cordial saludo, muy respetuosamente me permito informarles.

"Que el Fideicomiso Fondo Especial de Migración JADGME – BCR en el año 2020 adquirió mediante el proceso de licitación pública 2019PP-000068-0016200001, adquirió un sistema de documentos migratorios, para expedir los diferentes documentos que expide la Dirección General de Migración y Extranjeria de Costa Rica, entre ellos, pasaporte biométrico de policarbonato, además compra de equipos tecnológicos, libretas electrónicas de pasaportes biométricos de policarbonato, soporte y mantenimiento a la solución de personalización, a la empresa GSI-Veridos, el monto del contrato asciende a más de $9 millones de USD a la fecha.

Este contrato incluye suministro e implementación, servicios profesionales, equipos y **sistemas para la transición de pasaporte mecánicos (sin electrónica) a pasaporte electrónicos**. Mencionar que este contrato incluye un volumen mayor a 1.000,000 libretas de pasaportes electrónicos con página de policarbonato entregados a la fecha.

En la ejecución del contrato antes señalado, es importante indicar que, la empresa GSI-Veridos ha cumplido a satisfacción.

Cordialmente se suscribe de ustedes muy atentamente.

GESTIÓN MIGRACIONES

Rosibel Vargas Durán
Gestora
Gestión de Migraciones
rvargasd@migracion.go.cr

c.c. Archivo.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo. RD

812

REPÚBLICA DE COSTA RICA

MINISTERIO DE RELACIONES EXTERIORES Y CULTO

A-111106211

APOSTILLE

(Convention de La Haye du 5 octobre 1961)

1. País: Costa Rica
(Country – Pays:)

Código: RGDMCP3W5VR
(Code – Code:)

El presente documento público
(This public document – Le présent acte public)

2. Ha sido firmado por: Rosibel Vargas Duran
(Has been signed by – A été signé par:)

3. Actuando en calidad de: Gestor (a) de Migraciones
(Acting in the capacity of – Agissant en qualité de:)

4. Lleva el sello/estampilla de: Dirección General de Migración y Extranjería
(Bears the seal/stamp of – Est revêtu du sceau/timbre de:)

Certificado
(Certified – Attesté)

5. En: San José, Costa Rica
(At – A:)

6. El: 06/06/2024
(On – Le:)

7. Por: Ivannia Espinoza Rodriguez , Oficial de Autenticaciones
(By – Par:) Ministry of Foreign Affairs – Ministère des Affaires Étrangères

8. No.: 1101284
(Under number – Sous le numéro:)

9. Sello:
(Seal – Sceau:)

10. Firma:
(Signature – Signature:)

Esta apostilla / legalización sólo certifica la autenticidad de la firma, la capacidad del signatario y el sello o timbre que ostenta. Esta no certifica el contenido del documento para el cual se espidió.

This apostille / legalization only certifies the signature, the capacity of the signer and the seal or stamp it bears. It does not certify the content of the document for which it was issued.

Cette apostille / legalization ne certifie que la signature, la qualité en laquelle le signataire de l'acte a agi, et le sceau ou timbre dont cet acte est revêtu. Elle ne certifie pas le contenu du document pour lequel elle a été émise.

La autenticidad de esta apostilla / legalización puede ser verificada en: - The authenticity of this apostille / legalization may be verified at: - L'authenticité de cette apostille / legalization peut être vérifiée sur: http://www.rree.go.cr

1106211

Total Timbres: [illegible] 587.50

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

813

JOSÉ MIGUEL GUERRA GONZÁLEZ

Intérprete Judicial

Yo, José Miguel Guerra González, Intérprete Judicial del Juzgado de Primera Instancia del Distrito Nacional, República Dominicana, debidamente juramentado para el ejercicio de mis funciones, CERTIFICO: Que he traducido un documento escrito en inglés, portugués y alemán cuya versión en español, a mi mejor entender, es la siguiente:

Copia Certificada

REPÚBLICA DE MOZAMBIQUE

MINISTERIO DEL INTERIOR

DESPACHO DEL MINISTRO

Para

JUNTA CENTRAL ELECTORAL

Comisión de Compras y Contrataciones

Referencia: JCE-CCC-LPI-2024-0001

Ave. Gregorio Luperón esq. Ave. 27 de febrero,

Edificio Administrativo, ala este, 2do nivel

Las autoridades de Mozambique han adjudicado el contrato número 001/CP/MNT-DAF-UGEA/2017 para la prestación de servicios durante un periodo de ocho años y seis meses. El alcance del proyecto consiste en la entrega, distribución, instalación y ampliación de un sistema de última generación para la emisión de múltiples tipos de documentos de identificación a ciudadanos y visitantes, por un total de 92 millones de USD, con un contrato válido hasta el 03/2027.

A escala nacional, el gobierno emite tarjetas nacionales de identificación biométricas, documentos de viaje electrónicos y documentos biométricos de viaje de emergencia a todos los ciudadanos de Mozambique.

Las embajadas y los consulados también apoyan la emisión de documentos de viaje, tarjetas de identificación y documentos de emergencia para los ciudadanos mozambiqueños. Para los visitantes, se pueden emitir visados biométricos en todos los aeropuertos y puestos fronterizos, así como en los consulados y embajadas. Además, se emiten documentos de residencia para extranjeros y documentos de viaje de emergencia biométricos para extranjeros, así como documentos de viaje para refugiados.

Por la presente, el Ministerio del Interior de la República de Mozambique confirma que Mühlbauer [illegible] GmbH ha recibido el encargo de implantar un

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

sistema de emisión de documentos de identificación y un sistema de gestión de fronteras, que incluye:

- Diseño y suministro de tarjetas de identificación en policarbonato para el proyecto
- 10,400,000 tarjetas nacionales de identificación
- 120,000 documentos de residencia

Diseño y suministro de pasaportes electrónicos en policarbonato para el proyecto

- 1,200,000 pasaportes ordinarios;
- 6,400 pasaportes de servicio;
- 2,400 pasaportes diplomáticos;
- 22,400 pasaportes para refugiados;
- 80,000 documentos de viaje para trabajadores;
- diseño y suministro de visados para el proyecto;
- integración e implementación de un sistema centralizado de gestión de datos personales y biométricos;
- sistema central para la personalización de tarjetas de identificación y pasaportes, que incluye sistemas de gestión de la personalización y máquinas de personalización de tarjetas y pasaportes mediante grabado por láser y codificación por chip;
- sistema nacional de registro con 177 centros nacionales de registro y 45 consulados;
- sistema central de gestión de fronteras para gestionar los procesos de control fronterizo;
- sistema nacional de control fronterizo que comprende 205 sistemas de inspección para puestos fronterizos terrestres y aeropuertos;
- mantenimiento de todos los componentes instalados a nivel nacional e internacional (sistemas de registro, sistemas centrales, impresoras de tarjetas, impresoras de pasaportes, impresoras de visados, sistemas de servidores, sistemas de software);
- la tecnología instalada suministrada es operada por técnicos de las autoridades mozambiqueñas en diferentes sectores. El mantenimiento y el soporte técnico son proporcionados a nivel nacional (descentralizado y centralizado) e internacional (consulados) por un equipo de soporte técnico creado por Mühlbauer.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.
[Illegible]

El contrato se amplió para incluir otros componentes tecnológicos (por ejemplo, el sistema eVisa), que actualmente está activo.

Se confirma también la experiencia en

- Suministro de impresoras electrónicas de tarjetas de identificación en policarbonato.
- Suministro de tarjetas de identificación electrónicas en policarbonato.
- Transición de documentos de identificación mecánicos (no electrónicos) a documentos de identificación electrónicos.
- Integración de sistemas en el proyecto de identificación electrónica.

Mühlbauer cumplió todas nuestras expectativas en cuanto a cantidades y fecha de entrega exactamente según lo establecido y acordado en el contrato.

Nos complace confirmar el éxito de la cooperación con Mühlbauer ID Services GmbH, que nos ha asistido en todos los asuntos de forma flexible y orientada al cliente, y confirmar además que la empresa ha cumplido todas nuestras expectativas.

Maputo, el día 4 de junio de 2024
Secretario Permanente

[Firmado]
Victor Domingos Canhembra Júnior
(Técnico Superior N1)

[Sello: República de Mozambique - Ministerio del Interior - Despacho del Secretario Permanente]

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

8/6

La copia anterior corresponde al documento original.

Roding, 19 de junio de 2024

[Firmado]
Notaria
[Sello: Katharina Marchner, Notaria de Roding]

No. de archivo 91 E 206/2024

Por este medio certifico la autenticidad de la firma que precede de la **Notaria Katharina Marchner de Roding,**

así como la autenticidad del sello oficial añadido.

Además, certifico que la persona antes mencionada está legalmente autorizada a ejecutar este acto oficial.

Ratisbona, el 19 de junio de 2024
La Presidenta del Tribunal Regional
De orden

[Firmado]
Manuela Wanner
Oficial Judicial

[Sello: Tribunal Regional de Ratisbona, Baviera]

Desglose de Costos
Impuesto: 25.00 €
(según el Art. 1, Párrafo 1 de la Ley de Costos Judiciales Estatales (LJKostG), en conjunto con la Sección 4, Párrafo 1 de la Ley de Costos de la Administración Judicial (JVKostG), KV 13.10)

El documento que antecede fue traducido en Santo Domingo, capital de la República Dominicana, el día 26 de junio del año 2024, y está registrado en mis archivos como "Carta de Referencia (Mozambique) MÜHLBAUER ID SERVICES GMBH 20240726O1".

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

Lic. José Miguel Guerra González
Intérprete Judicial del Juzgado de Primera Instancia
República Dominicana

JOSÉ MIGUEL GUERRA GONZÁLEZ
Intérprete Judicial
Tralega Traducciones Legales, Intérpretes Judiciales
809-535-3011 / 809-535-6011 tralega.com info@tralega.com

Beglaubigte Ablichtung

47

REPÚBLICA DE MOÇAMBIQUE

MINISTÉRIO DO INTERIOR

GABINETE DO MINISTRO

A
JUNTA CENTRAL ELECTORAL
Comisión de Compras y Contrataciones
Referencia: JCE-COC-LPI-2024-0001
Gregorio Luperón Ave. esq. 27 de febrero Ave.,
Edificio administrativo, ala este, 2do nivel.

As autoridades Moçambicanas adjudicaram um contrato com o numero 001/CP/MNT-DAF-UGEA/2017.para Prestação de serviços por um periodo de oito anos e seis meses. O âmbito do projecto consiste na entrega, distribuição, instalação e ampliação de um sistema de ponta para emissão de múltiplos tipos de documentos de identificação para cidadãos e visitantes, com o montante total de 92 Milhões de USD, com um contrato válido até 03/2027.	Las autoridades de Mozambique han adjudicado el contrato número 001/CP/MNT-DAF-UGEA/2017 para la prestación de servicios durante un periodo de ocho años y seis meses. El alcance del proyecto consiste en la entrega, distribución, instalación y ampliación de un sistema de última generación para la emisión de múltiples tipos de documentos de identificación a ciudadanos y visitantes, por un total de 92 millones de USD, con un contrato válido hasta el 03/2027.
Numa base nacional, o governo faz a emissão de Bilhetes de Identificação nacional biométricos, documentos de viagem eletrónicos, bem como, documentos de viagem de emergência biométricos para todos os cidadãos moçambicanos.	A escala nacional, el gobierno emite tarjetas nacionales de identificación biométricas, documentos de viaje electrónicos y documentos biométricos de viaje de emergencia a todos los ciudadanos de Mozambique.
Nas embaixadas e consulados, é também apoiada a emissão de Documentos de Viagem, Bilhetes de Identidade e Documentos de Emergência para cidadãos moçambicanos. Para os visitantes os Vistos biométricos podem ser emitidos em todos os aeroportos e postos fronteiriços, bem como, nos consulados e embaixadas. Além disso, são emitidos Documentos de Residência para Estrangeiros e Documentos de Viagem de Emergência biométricos para Estrangeiros, bem como, Documentos de Viagem para Refugiados.	Las embajadas y los consulados también apoyan la emisión de documentos de viaje, tarjetas de identificación y documentos de emergencia para los ciudadanos mozambiqueños. Para los visitantes, se pueden emitir visados biométricos en todos los aeropuertos y puestos fronterizos, así como en los consulados y embajadas. Además, se emiten documentos de residencia para extranjeros y documentos de viaje de emergencia biométricos para extranjeros, así como documentos de viaje para refugiados.
Por este meio o Ministério do Interior da República de Moçambique, confirma que Mühlbauer ID Services GmbH foi encarregada da implementação de um	Por la presente, el Ministerio del Interior de la República de Mozambique confirma que Mühlbauer ID Services GmbH ha recibido el encargo de implementación

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo R.D.

sistema de emissão de documentos de identificação e de um sistema de gestão de fronteiras, nos quais inclui:	sistema de emisión de documentos de identificación y un sistema de gestión de fronteras, que incluye:
• Elaboração e fornecimento de bilhetes de identificação em policarbonato para o projeto • 10,400,000 Bilhetes de Identificação Nacionais • 120.000 Documentos de Residência	• Diseño y suministro de tarjetas de identificación en policarbonato para el proyecto • 10.400.000 tarjetas nacionales de identificación • 120.000 documentos de residencia
Elaboração e fornecimento de passaportes electrónicos em policarbonato para o projeto • 1,200,000 Passaportes Ordinários; • 6,400 Passaportes de Serviço; • 2,400 Passaportes Diplomáticos; • 22,400 Passaportes para Refugiados; • 80,000 Documentos de viagem para Trabalhadores; • a elaboração e o fornecimento de vistos para o projeto.	Diseño y suministro de pasaportes electrónicos en policarbonato para el proyecto • 1.200.000 pasaportes ordinarios; • 6.400 pasaportes de servicio; • 2.400 pasaportes diplomáticos; • 22.400 pasaportes para refugiados; • 80.000 documentos de viaje para trabajadores; • diseño y suministro de visados para el proyecto.
• Integração e implementação de um sistema central de gestão de dados pessoais e biométricos; • sistema central para a personalização de bilhetes de identificação e documentos de passaporte, que inclui sistemas de gestão da personalização e máquinas de personalização de bilhetes e passaportes baseadas na gravação a laser e na codificação de chips; • sistema de registo a nível nacional com 177 centros de registo nacionais e 45 consulados; • sistema central de gestão das fronteiras para gerir os processos de controlo fronteiriço; • sistema nacional de controlo fronteiriço composto por 205 sistemas de inspeção para postos fronteiriços terrestres e aeroportos.	• Integración e implantación de un sistema centralizado de gestión de datos personales y biométricos; • sistema central para la personalización de tarjetas de identificación y pasaportes, que incluye sistemas de gestión de la personalización y máquinas de personalización de tarjetas y pasaportes mediante grabado por láser y codificación por chip; • sistema nacional de registro con 177 centros nacionales de registro y 45 consulados; • sistema central de gestión de fronteras para gestionar los procesos de control fronterizo; • sistema nacional de control fronterizo que comprende 205 sistemas de inspección para puestos fronterizos terrestres y aeropuertos.
• Manutenção de todos os componentes instalados a nível nacional e internacional (sistemas de registo, sistemas centrais, impressoras de bilhetes, impressoras de passaportes, impressoras de vistos, sistemas de servidores, sistemas de software).	• Mantenimiento de todos los componentes instalados a nivel nacional e internacional (sistemas de registro, sistemas centrales, impresoras de tarjetas, impresoras de pasaportes, impresoras de visados, sistemas de servidores, sistemas de software).
• A tecnologia instalada fornecida é operada pelos técnicos das autoridades moçambicanas de diferentes sectores. A manutenção e a assistência técnica são prestadas a nível nacional (descentralizada e centralizada) e internacional (consulados) por uma equipa de assistência técnica criada pela Mühlbauer.	• La tecnología instalada suministrada es operada por técnicos de las autoridades mozambiqueñas en diferentes sectores. El mantenimiento y el soporte técnico son proporcionados a nivel nacional (descentralizado y centralizado) e internacional (consulados) por un equipo de soporte técnico creado por Mühlbauer.

819

O contrato celebrado foi alargado de modo a incluir outras componentes tecnológicas (por exemplo, o sistema eVisa) que se encontra em estado ativo. Confirmação ainda a experiência em • Fornecimento de impressoras electrónicas de bilhetes de identificação em policarbonato. • Fornecimento de bilhetes de identificação electrónicos em policarbonato. • Transição dos documentos de identificação mecânicos (não electrónicos) para os documentos de identificação electrónicos. • Integração dos sistemas no projeto de identificação electrónica. A Mühlbauer satisfez todas nossas expectativas em termos de quantidades e data de entrega exactamente como indicado e acordado no contrato. Confirmamos com satisfação a cooperação bem-sucedida com a Mühlbauer ID Services GmbH, a qual prestou-nos assistência em todas as questões de uma forma flexível e orientada para o cliente, e confirmamos ainda que a empresa cumpriu todas as nossas expectativas.	El contrato se amplió para incluir otros componentes tecnológicos (por ejemplo, el sistema eVisa), que actualmente está activo. Se confirma también la experiencia en • Suministro de impresoras electrónicas de tarjetas de identificación en policarbonato. • Suministro de tarjetas de identificación electrónicas en policarbonato. • Transición de documentos de identificación mecánicos (no electrónicos) a documentos de identificación electrónicos. • Integración de sistemas en el proyecto de identificación electrónica. Mühlbauer cumplió todas nuestras expectativas en cuanto a cantidades y fecha de entrega exactamente según lo establecido y acordado en el contrato. Nos complace confirmar el éxito de la cooperación con Mühlbauer ID Services GmbH, que nos ha asistido en todos los asuntos de forma flexible y orientada al cliente, y confirmar además que la empresa ha cumplido todas nuestras expectativas.

Maputo, aos 04 de Junho de 2024

O SECRETÁRIO PERMANENTE

VICTOR DOMINGOS CANHENGA JÚNIOR

(TECNICO SUPERIOR N1)

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

820

Die Ablichtung stimmt mit der Urschrift überein.
Roding, 19. JUNI 2024
T. Marchner
Notarin

Gz. 91 E 206/2024

Die Echtheit vorstehender Unterschrift von

Notarin Katharina Marchner in Roding

und die Echtheit des beigedrückten Dienstsiegels werden hiermit bestätigt.

Zugleich wird bescheinigt, dass der/die Vorgenannte zur Vornahme der Amtshandlung gesetzlich befugt war.

Regensburg, den 19. Juni 2024
Der Präsident des Landgerichts
Im Auftrag

Manuela Wanner
Justizangestellte

BAYERN LANDGERICHT REGENSBURG

Kostenrechnung
Gebühr: 25,00 €
(gem. Art. 1 Abs. 1 LJKostG, i.V.m. § 4 Abs. 1 JVKostG, KV 13.10

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

Consulado General
de la República Dominicana
en Frankfurt, Alemania

Stiftstr.2, 60313 Frankfurt am Main, Alemania.
Tel.:49 69 74 30 77 61 / Fax: 49 69 74 38 76 40
www.consuladodominicanofrm@hotmail.com

821

Reg.00285/2024

CONSULADO GENERAL DE LA REPUBLICA DOMINICANA EN FRANKFURT, ALEMANIA.

CERTIFICO Y DOY FE (sin entrar en el contenido del documento ni ulterior destino que pueda dársele): que la firma que aparece al pie de **ESTA COPIA NOTARIAL**, Identificado con el **No. S/N**, de fecha **19 DE JUNIO DEL 2024,** corresponde **A LA SRA. MANUELA WANNER, PRESIDENTE DE LA AUDIENCIA PROVINCIAL**, de la ciudad de REGENSBURG, Alemania.

Y que es la Firma que acostumbra a usar en todos sus actos y a la cual se debe entera fe y crédito.

En Frankfurt am Main, Alemania, a los veintiún (21) dias del mes de junio del año dos mil veinticuatro (2024).

Nivel Aurora Tapia Ortiz
Vicecónsul

CONSULADO GENERAL DE LA REPUBLICA DOMINICANA FRANKFURT, ALEMANIA

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

823

JOSÉ MIGUEL GUERRA GONZÁLEZ
Intérprete Judicial

Yo, José Miguel Guerra González, Intérprete Judicial del Juzgado de Primera Instancia del Distrito Nacional, República Dominicana, debidamente juramentado para el ejercicio de mis funciones, CERTIFICO: Que he traducido un documento escrito en español, inglés y alemán, cuya versión en español, a mi mejor entender, es la siguiente:

Copia certificada de un archivo PDF

[Escudo con texto en bengali]

Daca, 30 de mayo de 2024

Respetados Señores
Junta Central Electoral (JCE)
República Dominicana
Santo Domingo

Ref.: JCE-CCC-LPI-2024-0001 «Contratación de la empresa que se encargará de suplir los equipos, materiales y servicios para la impresión de la nueva Cédula de Identidad y Electoral (CIE) y Cédula de Identidad (CI)».

Respetados Señores:

El Departamento de Inmigración y Pasaportes de la República Popular de Bangladesh certifica que la empresa **Veridos GmbH**, con número de Registro de Contribuyente 143/306/40066, proporcionó el servicio bajo el contrato No. 58.01.0000.101.14.003.17.1343 para el suministro e implementación, servicios profesionales, equipos y sistemas para la transición de Pasaportes Legibles por Máquina (MRP) a documentos de identificación electrónicos (Pasaportes Electrónicos), por un término de 13 millones de unidades dese 2020 hasta 2024 (últimos 4 años). Es importante mencionar que este contrato incluye un volumen mayor a 1,000,000 de documentos de identificación por año.

En la ejecución del contrato mencionado anteriormente, afirmamos que el rendimiento de la empresa Veridos GmbH ha cumplido nuestras expectativas razón por lo que expresamos nuestra satisfacción y los recomendamos para ejecutar el proyecto en referencia.

Atentamente,

[Firmado] 30/05/24
Nombre: MOHAMMAD NURUS SALAM
Cargo: General de Brigada (Director de Proyecto)
Teléfono: +8801769050500
Correo electrónico: pd.e-passport@passport.gov.bd
Institución: Proyecto de Gestión de Pasaportes Electrónicos y Control Fronterizo Automatizado
Departamento of Inmigración & Pasaportes

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

824

Yo, Notario Público, por la presente certifico que este documento es una copia fiel de un archivo PDF.

Múnich, el 04/06/2024

[Firmado]
Dr. Bernhard Schaub
Notario Público de Múnich

[Sello en relieve: Dr. Bernhard Schaub, Notario de Múnich]

Por este medio certifico la autenticidad de la firma que precede del notario Dr. Bernhard Schaub así como la autenticidad del sello oficial añadido.

Además, certifico que la persona antes mencionada está autorizada a ejecutar este acto oficial.

Múnich, el 6 de junio de 2024
La Presidenta del Tribunal Regional de Múnich I
De orden

[Firmado]
Lea Adelsberger
Secretaria del Tribunal

[Sello: Tribunal Regional de Múnich I, Baviera]

El documento que antecede fue traducido en Santo Domingo, capital de la República Dominicana, el día 26 de julio del año 2024, y está registrado en mis archivos como "Carta de Referencia (Bangladesh) VERIDOS GMBH 2024072601".

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

Lic. José Miguel Guerra González
INTÉRPRETE JUDICIAL DEL JUZGADO DE PRIMERA INSTANCIA
República Dominicana

JOSÉ MIGUEL GUERRA GONZÁLEZ
Intérprete Judicial
Tralega Traducciones Legales, Intérpretes Judiciales
809-535-3011 / 809-535-6011 tralega.com info@tralega.com

CERTIFIED COPY OF A PDF-FILE

215

Dhaka, May 30, 2024./ *Dhaka, 30 de Mayo de 2024.*

Respected / *Respetados*
Gentlemen / *Señores*
Central Electoral Board (JCE) / *Junta Central Electoral (JCE)*
Dominican Republic / *República de Dominicana*
Santo Domingo / *Santo Domingo*

Ref: JCE-CCC-LPI-2024-0001 "Hiring of the company that will supply the equipment, materials and services for the printing of the new Identity and Electoral Card (CIE) and Identity Card (CI)". / *Ref: JCE-CCC-LPI-2024-0001 «Contratación de la empresa que se encargará de suplir los equipos, materiales y servicios para la impresión de la nueva Cédula de Identidad y Electoral (CIE) y Cédula de Identidad (CI)».*

Respected Gentlemen / *Respetados Señores:*

Department of Immigration and Passport of the People Republic of Bangladesh certifies that the company **Veridos GmbH**, with Taxpayer Registration No. 143/306/40066, provided the service under contract No. Contract No:58.01.0000.101.14.003.17.1343 for the supply and implementation, professional services, equipment and systems for the transition from Machine Readable Passports(MRP) to electronic identification documents (electronic Passports), for a term of 13 million units from 2020 to 2024 (last 4 years). It is important to mention that this contract includes a volume greater than 1,000,000 identification documents per year. / *El Departamento de Inmigración y Pasaportes de la República Popular de Bangladesh certifica que la empresa **Veridos GmbH**, con número de registro de contribuyente 143/306/40066, proporcionó el servicio bajo el contrato No. Contract No:58.01.0000.101.14.003.17.1343 para el suministro e implementación, servicios profesionales, equipos y sistemas para la transición de Pasaportes Legibles por Máquina (MRP) a documentos de identificación electrónicos (Pasaportes Electrónicos), por un término de 13 millones de unidades desde 2020 hasta 2024 (últimos 4 años). Es importante mencionar que este contrato incluye un volumen mayor a 1,000,000 de documentos de identificación por año.*

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

824

In the execution of the contract mentioned above, we state that the performance of the company **Veridos GmbH**, has met the highest expectations, which is why we express our satisfaction, and recommend d to execute the project in reference. / *En la ejecución del contrato mencionado anteriormente, afirmamos que el rendimiento de la empresa **Veridos GmbH** ha cumplido nuestras expectativas razón por lo que expresamos nuestra satisfacción y recomendamos ejecutar el proyecto en referencia.*

Sincerely/ *Atentamente*,

30.05.24

Name / *Nombre*: **MOHAMMAD NURUS SALAM**
Position / *Cargo*: Brigadier General (Project Director)
Phone / *Teléfono*:+8801769050500
Email / *Correo electrónico*: pd.e-passport@passport.gov.bd
Institution / *Institución*: e-Passport and Automated Border Control Management Project
Department of Immigration & Passports.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

227

I, Notary Public, hereby certify that this document is a true copy of a pdf-file.

Munich, this 04.06.2024

Dr. Bernhard Schaub
Notary Public in Munich

Die Echtheit vorstehender Unterschrift des Notars Dr. Bernhard Schaub und die Echtheit des beigedrückten Dienstsiegels werden hiermit bestätigt.
Zugleich wird bescheinigt, dass der Vorgenannte zur Vornahme der Amtshandlung befugt war.

München, 06. Juni 2024
Die Präsidentin des Landgerichts München I
Im Auftrag

Justizsekretärin

828

EMBAJADA DE LA REPÚBLICA DOMINICANA
EN ALEMANIA
SECCIÓN CONSULAR

CERTIFICO, que la firma que aparece al pie de esta documentación es la del/ de la Sr./a. Adelsberger - Justicia Regional
CIUDAD Muenchen y que es la misma que acostumbra a usar en todos sus actos y la cual es de su entera fé y crédito.
FECHA 13.06.2024

HEIDI TAVERAS
CONSEJERA

EMBAJADA DE LA REPÚBLICA DOMINICANA BERLÍN, ALEMANIA

CONSORCIO EMDOC
EMDOC CONSORCIO
Santo Domingo, RD

829

República Dominicana

MINISTERIO DE RELACIONES EXTERIORES

Viceministerio para Asuntos Consulares y Migratorios

Dirección de Legalización de Documentos

APOSTILLA

(Convention de la Haye du 5 octobre 1961)

1.País:
Country / Pays: REPÚBLICA DOMINICANA

El presente documento público
This public document / Le présent acte public

2.Ha sido firmado por:
Has been signed by / A été signé par: HEIDI GABRIELA TAVERAS MORILLO

3.Quien actúa en calidad de:
Acting in the capacity of / Agissant en qualité de: CONSEJERA

4.Y está revestido del sello / timbre de:
Bears the seal / stamp of
Est revêtu du sceau / timbre de: EMBAJADA DE LA REPUBLICA DOMINICANA EN LA REPUBLICA FEDERAL DE ALEMANIA

Certificado
Certified / Attesté

5.En: Al / À	SANTO DOMINGO	**6.El día:** The / Le	28/7/2024
7.Por: By / Par	OPINIO ANTONIO DIAZ VARGAS - VICEMINISTRO ASUNTOS CONSULARES Y MIGRATORIOS	**8.Bajo el número:** N° / Sous°	AP-2024-7-28-21
9.Sello / Timbre: Seal / Stamp Sceau / Timbre		**10.Firma:** Signature	

Verificación
Verification / Vérification

País Destino:	REPÚBLICA DOMINICANA	**Código de verificación:**	ACYQYKWMDJF9WX9

Esta Apostilla certifica únicamente la autenticidad de la firma, la calidad en que el signatario del documento haya actuado, y en su caso, la identidad del sello o timbre del que el documento público esta revestido.

This Apostille only certifies the authenticity of the signature and the capacity of the person who has signed the public document, and, where appropriate, the identity of the seal or stamp which the public document bears.

Cette Apostille atteste uniquement la véracité de la signature, la qualité en laquelle le signataire de l'acte a agi et, le cas échéant, l'identité du sceau ou timbre dont cet acte public est revêtu.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

830

JOSÉ MIGUEL GUERRA GONZÁLEZ

Intérprete Judicial

Yo, José Miguel Guerra González, Intérprete Judicial del Juzgado de Primera Instancia del Distrito Nacional, República Dominicana, debidamente juramentado para el ejercicio de mis funciones, CERTIFICO: Que he traducido un documento escrito en francés, español, inglés y alemán, cuya versión en español, a mi mejor entender, es la siguiente:

Copia certificada de un archivo PDF

República de Haití
Ministerio del Interior y las Comunidades Territoriales

No. _____

Ciudad de Puerto Príncipe, 14 de Mayo de 2024
Jean Osselin LAMBERT, Ing. Director
Ministerio del Interior y las Comunidades Territoriales (MICT)
171, Avenue John Brown, Lalue, Puerto Príncipe, Haití

Respetados Señores
Junta Central Electoral (JCE)
República de Dominicana
Santo Domingo

Ref.: JCE-CCC-LPI-2024-0001 «Contratación de la empresa que se encargará de suplir los equipos, materiales y servicios para la impresión de la nueva Cédula de Identidad y Electoral (CIE) y Cédula de Identidad (CI)».

Respetados Señores:

El Ministerio del Interior y las Comunidades Territoriales de Haití (MICT), certifica que la empresa Veridos GmbH, con Registro de Contribuyente No. 143/306/40066, prestó el servicio bajo contrato No. BGB/PB/1112 No. 000942 para el suministro e implementación, servicios profesionales, equipos y sistemas para la transición de documentos de identificación mecánicos (no electrónicos) a documentos de identificación electrónicos, en un término de 6,000,000 de unidades desde el 2019 hasta el 2025 (últimos 5 años), es importante mencionar que este contrato incluye un volumen mayor a 1,000,000 de documentos de identificación al año.

En la ejecución del contrato antes señalado, manifestamos que el desempeño de la empresa Veridos GmbH, ha cumplido con las más altas expectativas, por lo que manifestamos nuestra satisfacción, y recomendamos a este proponente ya que consideramos que está plenamente facultado para ejecutar el proyecto en referencia.

Atentamente,

[Firmado]
Nombre: Jean Osselin LAMBERT
Cargo: Ing. Director
Teléfono: +50931703734
Correo electrónico: jeanosselin.lambert@mict.gouv.ht
Institución: Ministerio del Interior y las Comunidades Territoriales (MICT)

[Sello: Ministerio del Interior y las Comunidades Territoriales - DIE - Dirección de Inmigración]

[Sello: Ministerio del Interior y las Comunidades Territoriales - MICT/DTIC - Dirección de Tecnologías de la Información y las Comunicaciones]

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

831

Yo, Notario Público, por la presente certifico que este documento es una copia fiel de un archivo PDF.

Múnich, el 04/06/2024

[Firmado]
Dr. Bernhard Schaub
Notario de Múnich

[Sello en relieve: Dr. Bernhard Schaub, Notario de Múnich]

Por este medio certifico la autenticidad de la firma que precede del notario Dr. Bernhard Schaub así como la autenticidad del sello oficial añadido.

Además certifico que la persona antes mencionada está autorizada a ejecutar este acto oficial.

Múnich, el 6 de junio de 2024
La Presidenta del Tribunal Regional de Múnich I
De orden

[Firmado]
Lea Adelsberger
Secretaria del Tribunal

[Sello: Tribunal Regional de Múnich I, Baviera]

El documento que antecede fue traducido en Santo Domingo, capital de la República Dominicana, el día 26 de julio del año 2024, y está registrado en mis archivos como "Carta de Referencia (Haití) VERIDOS GMBH 2024072601".

CONSORCIO EMDOC
EMDOC CONSORCIO
Santo Domingo, R.D.

Lic. José Miguel Guerra González
INTÉRPRETE JUDICIAL DEL JUZGADO DE PRIMERA INSTANCIA
República Dominicana

JOSÉ MIGUEL GUERRA GONZÁLEZ
Intérprete Judicial
Tralego Traducciones Legales, Intérpretes Judiciales
809-535-3011 / 809-535-6011 tralego.com info@tralego.com

CERTIFIED COPY OF A PDF-FILE

832

RÉPUBLIQUE D'HAÏTI

MINISTÈRE DE L'INTÉRIEUR ET DES COLLECTIVITÉS TERRITORIALES

No. .....

City of Port au Prince , May 14 th, 2024/ *Ciudad de Puerto Príncipe, 14 de Mayo de 2024*
Jean Osselin LAMBERT, Ing Directeur / *Jean Osselin LAMBERT, Ing Director*
Ministère de l'Intérieur et des Collectivités Territoriales (MICT) / *Ministerio del Interior y de las Colectividades Territoriales (MICT)*
171, Avenue John Brown / Lalue /*171, Avenue John Brown / Lalue*
Port-au-Prince / Haïti / *Port-au-Prince / Haití*

Respected / *Respetados*
Gentlemen / *Señores*
Central Electoral Board (JCE) / *Junta Central Electoral (JCE)*
Dominican Republic / *República de Dominicana*
Santo Domingo / *Santo Domingo*

Ref: JCE-CCC-LPI-2024-0001 "Hiring of the company that will supply the equipment, materials and services for the printing of the new Identity and Electoral Card (CIE) and Identity Card (CI)". / *Ref: JCE-CCC-LPI-2024-0001 «Contratación de la empresa que se encargará de suplir los equipos, materiales y servicios para la impresión de la nueva Cédula de Identidad y Electoral (CIE) y Cédula de Identidad (CI)».*

Respected Gentlemen / *Respetados Señores:*

Ministry of Interior and Territorial Communities of Haiti (MICT) certifies that the company Veridos GmbH, with Taxpayer Registration No. 143/306/40066 , provided the service under contract No. BGB/PB/1112 No.000942 for **the supply and implementation, professional services, equipment and systems for the transition from mechanical (non-electronic) identification documents to electronic identification documents, for a term of 6.000.000 Units from 2019 to 2025 (last 5 years).** It is important to mention that this contract includes a volume greater than 1,000,000 identification documents per year. / ***Ministerio del Interior y de las Comunidades Territoriales de Haití (MICT), certifica que la empresa Veridos GmbH, con Registro de Contribuyente No. 143/306/40066, prestó el servicio bajo contrato No. BGB/PB/1112 No.000942 para el suministro e implementación, servicios profesionales, equipos y sistemas para la transición de documentos de identificación mecánicos (sin electrónica) a documentos de identificación electrónicos con***

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

un termino de 6.000.000 unidades a partir del 2019 hasta 2025 (últimos 5 años). *es importante mencionar que este contrato incluye un volumen mayor a 1,000,000 de documentos de identificación al año.*

In the execution of the contract mentioned above, we state that the performance of the company **Veridos GmbH**, has met the highest expectations, which is why we express our satisfaction, and recommend this proposer as we consider that they are fully empowered to execute the project in reference / *En la ejecución del contrato antes señalado, manifestamos que el desempeño de la empresa* ***Veridos GmbH,*** *ha cumplido con las más altas expectativas, por lo que manifestamos nuestro recibido a sastifacción, y recomendamos a este proponente ya que consideramos que está plenamente facultado para ejecutar el proyecto en referencia*

Sincerely/ *Atentamente*,

DIE

MICT/DTIC

Name / *Nombre*: Jean Osselin LAMBERT
Position / *Cargo*: Ing Directeur
Phone / *Teléfono*: +50931703734
Email / *Correo electrónico*: jeanosselin.lambert@mict.gouv.ht
Institution / *Institución*: Ministère de l'Intérieur et des Collectivités Territoriales (MICT)

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

834

I, Notary Public, hereby certify that this document is a true copy of a pdf-file.

Munich, this 04.06.2024

Dr. Bernhard Schaub
Notary Public in Munich

Die Echtheit vorstehender Unterschrift des Notars Dr. Bernhard Schaub und die Echtheit des beigedrückten Dienstsiegels werden hiermit bestätigt.
Zugleich wird bescheinigt, dass der Vorgenannte zur Vornahme der Amtshandlung befugt war.

München, 06. Juni 2024
Die Präsidentin des Landgerichts München I
Im Auftrag

Lea Adelsberger
Justizsekretärin

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

335

EMBAJADA DE LA REPÚBLICA DOMINICANA
EN ALEMANIA
SECCIÓN CONSULAR

CERTIFICO, que la firma que aparece al pie de esta documentación es la del/ de la Sr./a. Adelsberger - Justicia Regional
CIUDAD Munich y que es la misma que acostumbra a usar en todos sus actos y la cual es de su entera fé y crédito.
FECHA 13.06.2024

HEIDI TAVERAS

EMBAJADA DE LA REPÚBLICA DOMINICANA BERLÍN, ALEMANIA

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

836

República Dominicana
MINISTERIO DE RELACIONES EXTERIORES
Viceministerio para Asuntos Consulares y Migratorios
Dirección de Legalización de Documentos

APOSTILLA

(Convention de la Haye du 5 octobre 1961)

1.País:
Country / Pays: REPÚBLICA DOMINICANA

El presente documento público
This public document / Le présent acte public

2.Ha sido firmado por:
Has been signed by / A été signé par: HEIDI GABRIELA TAVERAS MORILLO

3.Quien actúa en calidad de:
Acting in the capacity of / Agissant en qualité de: CONSEJERA

4.Y está revestido del sello / timbre de:
Bears the seal / stamp of
Est revêtu du sceau / timbre de: EMBAJADA DE LA REPUBLICA DOMINICANA EN LA REPUBLICA FEDERAL DE ALEMANIA

Certificado
Certified / Attesté

5.En: At / À	SANTO DOMINGO	**6.El día:** The / Le	26/7/2024
7.Por: By / Par	OPINIO ANTONIO DIAZ VARGAS - VICEMINISTRO ASUNTOS CONSULARES Y MIGRATORIOS	**8.Bajo el número:** N° / Sous*	AP-2024-7-26-19
9.Sello / Timbre: Seal / Stamp Sceau / Timbre		**10.Firma:** Signature	

Verificación
Verification / Vérification

País Destino:	REPÚBLICA DOMINICANA	**Código de verificación:**	4WCHQE4G76TPMTV

Esta Apostilla certifica únicamente la autenticidad de la firma, la calidad en que el signatario del documento haya actuado, y en su caso, la identidad del sello o timbre del que el documento público sea revestido.

This Apostille only certifies the authenticity of the signature and the capacity of the person who has signed the public document, and, where appropriate, the identity of the seal or stamp which the public document bears.

Cette Apostille atteste uniquement la véracité de la signature, la qualité en laquelle le signataire de l'acte a agi et, le cas échéant, l'identité du sceau ou timbre dont cet acte public est revêtu.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

237

Experiencia en integración de sistemas, en un proyecto de identificación electrónica

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

iQtek · Müllbauer · GSI · ULTRATECH · VERIDOS

Ave. 27 de febrero esquina Ave. Tiradentes, Torre Feuaz, Local 6-B
Santo Domingo, Rep. Dominicana. Tel. (809) 412-5312

338

REGISTRO NACIONAL DE
LAS PERSONAS NATURALES

San Salvador, 30 de mayo 2024

RNPN-PRE-156/2024

JUNTA CENTRAL ELECTORAL
Comisión de Compras y Contrataciones
Referencia: JCE-CCC-LPI-2024-0001
Gregorio Luperón Ave. esq. 27 de febrero Ave.,
Edificio administrativo, ala este, 2do nivel

Reciba a través del presente un cordial saludo y mis más sinceros deseos de éxitos en el desempeño de sus funciones.

Por la presente, confirmamos que se encargó a Mühlbauer ID Services GmbH la modernización del actual sistema de emisión de documentos de identidad y de los documentos de identidad móviles a partir del primero de julio de 2021 mediante el contrato No. DR-CAFTA 02/2020. El alcance del trabajo y de la asignación es el siguiente:

- Diseño, fabricación y suministro de una nueva versión del documento de identidad en policarbonato (aprox. 8,493,685).
- Suministro de 22 nuevos sistemas de personalización de tarjetas Mühlbauer SCP 60 y su instalación.
- Integración y puesta en marcha de un sistema de gestión de la personalización a escala nacional, que suministra a los sistemas de personalización de tarjetas los datos de personalización necesarios.
- Suministro de identificaciones móviles, disponibles en dispositivos móviles Android e IOS.
- Mantenimiento de los sistemas desde su puesta en servicio, hasta 2027.

Nos complace confirmar por la presente la exitosa colaboración con Mühlbauer ID Services GmbH, que nos ha proporcionado soporte en todas las cuestiones de forma flexible y orientada al cliente, y confirmamos además que la empresa ha cumplido todas nuestras expectativas; a la vez, confirmamos la experiencia en:

- Suministro de identificaciones digitales o identidades móviles (Mobile ID)
- Suministro de integración de sistemas de un proyecto de identificación electrónica

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

Dirección: Ave. Manuel Enrique Araujo, Edificio Carbonell No.1, Col. Roma, San Salvador, San Salvador
Correo electrónico: presidencia.rnpn@rnpn.gob.sv
Teléfono: 2521-9630

REGISTRO NACIONAL DE
LAS PERSONAS NATURALES

Sin más sobre el particular, aprovecho la ocasión para reiterarle las muestras de mi consideración y estima.

DIOS, UNIÓN, LIBERTAD

Lic. Fernando José Velasco Aguirre
Presidente - Registrador Nacional
Tel. +503 2521 9338
Email: fernando.velasco@rnpn.gov.sv

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

840

MINISTERIO DE RELACIONES EXTERIORES

APOSTILLE

Convention de La Haye du 5 octobre 1961

1.País / Country / Pays: **El SALVADOR**

El Presente documento público / This Public document / Le présent acte public

2.Ha sido firmado por / Has been signed by / A été signé par: **FERNANDO JOSÉ VELASCO AGUIRRE**

3.Quien actúa en calidad de / Acting in the capacity of / Agissant en qualité de: **PRESIDENTE REGISTRADOR NACIONAL**

4.Y está revestido del sello / timbre de / Bears the seal/stamp of / Est revêtu du sceau / timbre de: **REGISTRO NACIONAL DE LAS PERSONAS NATURALES- RNPN**

Certificado / Certified / Attesté

5. En / at / à: **MINISTERIO DE RELACIONES EXTERIORES**

6.El día / the / le: **04/06/2024**

7. Por / by / par: **JEFE DE SECCIÓN DIRECCION GENERAL DEL SERVICIO EXTERIOR**

8.Bajo el número / No. / Sous No.: **79-2024-2761823-15991**

Tipo de documento/ Type of document/ Type du document: **CERTIFICACION**

Número de hojas que contiene el documento/ Number of sheets contained in the document/ Nombre de feuilles contenues dans le document: **1**

Esta Apostilla certifica únicamente la autenticidad de la firma, la calidad en que el signatario del documento haya actuado y, en su caso, la identidad del sello o timbre del que el documento público esté revestido. Esta Apostilla no certifica el contenido del documento para el cual se expidió.

This Apostille only certifies the authenticity of the signature and the capacity of the person who has signed the public document, and, where appropriate, the identity of the seal or stamp which the public document bears. This Apostille does not certify the content of the document for which it was issued.

Cette Apostille atteste uniquement la véracité de la signature, la qualité en laquelle le signataire de l'acte a agi et, le cas échéant, l'identité du sceau ou timbre dont cet acte public est revêtu. Cette Apostille ne certifie pas le contenu du document pour lequel elle a été émise.

EXONERADO DE DERECHOS CONSULARES

9. Sello (timbre) / Seal (stamp) / Sceau (timbre)

JOSE RAMÓN ZAPATA PORTILLO

10. Firma / Signature / Signature

CONSORCIO EMDOC, EMDOC CONSORCIO, Santo Domingo, R.D.

847

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

178

MINISTERIO DE GOBERNACIÓN Y POLICÍA / DIRECCIÓN GENERAL DE MIGRACIÓN Y EXTRANJERÍA | GOBIERNO DE COSTA RICA

842

San José, Costa Rica, 22 de mayo de 2024.
GM-112-06-2024

Señores
Junta Central Electoral (JCE)
República de Dominicana
Su Oficina.

Ref: JCE-CCC-LPI-2024-0001 «Contratación de la empresa que se encargará de suplir los equipos, materiales y servicios para la impresión de la nueva Cédula de Identidad y Electoral (CIE) y Cédula de Identidad (CI)».

Estimados señores:

Después de expresarles un cordial saludo, muy respetuosamente, me permito informarle.

"Que mediante el Fideicomiso Fondo Especial de Migración JADGME – BCR en el año 2020, se tramitó el proceso de licitación pública 2019PP-000068-0016200001 Pasaporte Biométrico, para adquirir un sistema de emisión de documentos migratorios, para la Dirección General de Migración de Costa Rica, entre ellos, pasaportes biométrico de policarbonato, también la compra de equipos tecnológicos, libretas electrónicas de pasaportes biométricos de policarbonato y soporte y mantenimiento a la solución; a través de la empresa GSI-Veridos, el monto del contrato asciende a más de $9 millones de USD a la fecha".

Este contrato incluyó **la integración de sistemas de información de la DGME**, servicios profesionales, implementación, suministro de impresoras y sistemas para la transición del pasaporte mecánico (sin electrónica) a pasaporte electrónico, mencionar que este contrato incluye más de un 1,000,000 libretas de pasaportes electrónicos con página de policarbonato entregados a la fecha.

En la ejecución del contrato antes señalado, es importante indicar que, la empresa GSI-Veridos ha cumplido a satisfacción.

Cordialmente se suscribe de ustedes muy atentamente,

GESTIÓN

Rosibel Vargas Durán
Gestora
Gestión de Migraciones, DGME.
rvargasd@migracion.go.cr

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

C.C. Archivo.

MINISTERIO DE GOBERNACIÓN Y POLICÍA / DIRECCIÓN GENERAL DE MIGRACIÓN Y EXTRANJERÍA | GOBIERNO DE COSTA RICA

843

REPÚBLICA DE COSTA RICA

MINISTERIO DE RELACIONES EXTERIORES Y CULTO

A-1106210

APOSTILLE

(Convention de La Haye du 5 octobre 1961)

1. País: Costa Rica
(Country – Pays:)

Código: RGDLSPZJWZB
(Code – Code:)

El presente documento público
(This public document – Le présent acte public)

2. Ha sido firmado por: Roaibel Vargas Duran
(Has been signed by – A été signé par:)

3. Actuando en calidad de: Gestor (a) de Migraciones
(Acting in the capacity of – Agissant en qualité de:)

4. Lleva el sello/estampilla de: Dirección General de Migración y Extranjería
(Bears the seal/stamp of – Est revêtu du sceau/timbre de:)

Certificado
(Certified – Attesté)

5. En: San José, Costa Rica
(At – A:)

6. El: 06/06/2024
(On – Le)

7. Por: Ivannia Espinoza Rodriguez , Oficial de Autenticaciones
(By – Par:) Ministry of Foreign Affairs – Ministère des Affaires Étrangères

8. No.: 1101283
(Under number – Sous le numéro:)

9. Sello:
(Seal – Sceau:)

10. Firma:
(Signature – Signature)

1106210

Esta apostilla / legalización sólo certifica la autenticidad de la firma, la capacidad del signatario y el sello o timbre que ostenta. Ésta no certifica el contenido del documento para el cual se expidió.

This apostille / legalization only certifies the signature, the capacity of the signer and the seal or stamp it bears. It does not certify the content of the document for which it was issued.

Cette apostille / legalization ne certifie que la signature, la qualité en laquelle le signataire de l'acte a agi, et le sceau/timbre dont cet acte est revêtu. Elle ne certifie pas le contenu du document pour lequel elle a été émise.

La autenticidad de esta apostilla / legalización puede ser verificada en: - The authenticity of this apostille / legalization may be verified at: - L'authenticité de cette apostille / legalization peut être vérifiée sur: http://www.rree.go.cr

CONSORCIO EMDOC
EMDOC CONSORCIO
Santo Domingo, R.D.

3.1.6.3 Requisitos de experiencia (no obligatorios)



847

Requisitos de experiencia (no obligatorios)

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

Experiencia en distintos clientes y países, en cédulas digital o identidades móviles (Mobile ID

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, RD

846

REGISTRO NACIONAL DE
LAS PERSONAS NATURALES

San Salvador, 13 de junio 2024

RNPN-PRE-160/2024

JUNTA CENTRAL ELECTORAL
Comisión de Compras y Contrataciones
Referencia: JCE-CCC-LPI-2024-0001
Gregorio Luperón Ave. esq. 27 de febrero Ave.,
Edificio administrativo, ala este, 2do nivel.

Reciba a través del presente un cordial saludo y mis más sinceros deseos de éxitos en el desempeño de sus funciones.

Por la presente confirmamos que se encargó a Mühlbauer ID Services GmbH la modernización del actual sistema de emisión de documentos de identidad y de los documentos de identidad móviles en julio de 2021 mediante el contrato No. DR-CAFTA 02/2020. El alcance del trabajo y de la asignación fueron los siguientes:

- Diseño, fabricación y suministro de una nueva versión del documento de identidad en policarbonato (aprox. 8,493,685).
- Suministro de 22 nuevos sistemas de personalización de tarjetas Mühlbauer SCP 60 y su instalación.
- Integración y puesta en marcha de un sistema de gestión de la personalización a escala nacional, que suministra a los sistemas de personalización de tarjetas los datos de personalización necesarios.
- Suministro de al menos 100.000 identificaciones móviles conformes a la norma ISO 18013-5, disponibles en dispositivos móviles Android e IOS.
- Mantenimiento de los sistemas desde su puesta en servicio, hasta 2027.

Nos complace confirmar por la presente la exitosa colaboración con Mühlbauer ID Services GmbH, quien nos ha proporcionado soporte en todas las cuestiones de forma flexible y orientada al cliente, y confirmamos además que la empresa ha cumplido todas nuestras expectativas; a la vez, confirmamos la experiencia en:

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

Dirección: Ave. Manuel Enrique Araujo, Edificio Carbonell No.1, Col. Roma, San Salvador, San Salvador
Correo electrónico: presidencia.rnpn@rnpn.gob.sv
Teléfono: 2521-9630

REGISTRO NACIONAL DE
LAS PERSONAS NATURALES

- el suministro de identificaciones digitales o identidades móviles (Mobile ID)
- el suministro de integración de sistemas de un proyecto de identificación electrónica

Sin más sobre el particular, aprovecho la ocasión para reiterarle las muestras de mi consideración y estima.

Lic. Fernando José Velasco Aguirre
Presidente - Registrador Nacional
Tel. +503 2521 9338
Email: fernando.velasco@rnpn.gov.sv

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

8 4 8

MINISTERIO DE RELACIONES EXTERIORES

APOSTILLE

Convention de La Haye du 5 octobre 1961

1.País / Country / Pays: **El SALVADOR**

El Presente documento público / This Public document / Le présent acte public

2.Ha sido firmado por / Has been signed by / A été signé par: **FERNANDO JOSÉ VELASCO AGUIRRE**

3.Quien actúa en calidad de / Acting in the capacity of / Agissant en qualité de: **PRESIDENTE REGISTRADOR NACIONAL**

4.Y está revestido del sello / timbre de / Bears the seal/stamp of / Est revêtu du sceau / timbre de: **REGISTRO NACIONAL DE LAS PERSONAS NATURALES- RNPN**

Certificado / Certified / Attesté

5. En / at / à: **MINISTERIO DE RELACIONES EXTERIORES**

6.El día / the / le: **13/06/2024**

7. Por / by / par: **JEFE DE SECCIÓN DIRECCION GENERAL DEL SERVICIO EXTERIOR**

8.Bajo el número / No. / Sous No.: **79-2024-2778065-17175**

Tipo de documento/ Type of document/ Type du document: **CERTIFICACION**

Número de hojas que contiene el documento/ Number of sheets contained in the document/ Nombre de feuilles composant dans le document: **1**

Esta Apostilla certifica únicamente la autenticidad de la firma, la calidad en que el signatario del documento haya actuado y, en su caso, la identidad del sello o timbre del que el documento público esté revestido. Esta Apostilla no certifica el contenido del documento para el cual se expidió.

This Apostille only certifies the authenticity of the signature and the capacity of the person who has signed the public document, and, where appropriate, the identity of the seal or stamp which the public document bears. This Apostille does not certify the content of the document for which it was issued.

Cette Apostille atteste uniquement la véracité de la signature, la qualité en laquelle le signataire de l'acte a agi et, le cas échéant, l'identité du sceau ou timbre dont cet acte public est revêtu. Cette Apostille ne certifie pas le contenu du document pour lequel elle a été émise.

EXONERADO DE DERECHOS CONSULARES

9. Sello (Timbre) / Seal (Stamp) / Sceau (timbre):

10. Firma / Signature / Signature:

JOSE RAMÓN ZAPATA PORTÍLLO

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D

849

Experiencia de haber operado un proyecto de impresión de soluciones, al menos doscientas (200) impresoras distribuidas nacional e internacional (fuera del país).

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

Beglaubigte Ablichtung 350

Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

Director Comercial
José Miguel Fernández de Liencres

JUNTA CENTRAL ELECTORAL
Comisión de Compras y Contrataciones
Referencia: JCE-CCC-LPI-2024-0001
Gregorio Luperón Ave. esq. 27 de febrero Ave.,
Edificio administrativo, ala este, 2do nivel.
Santo Domingo / Dominican Republic

Madrid a, 05 de septiembre de 2024

Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda (FNMT-RCM) ha estado utilizando, entre otros, tecnología y maquinaria de alta gama de Mühlbauer para la producción y personalización de DNI electrónicos, así como muchos otros productos y proyectos, cumpliendo nuestras expectativas en términos de calidad, servicio y asistencia técnica.
A partir de 2006, los DNI españoles se empezaron a personalizar con equipos de Mühlbauer.
Mühlbauer entregó desde 2006 la cantidad de 324 máquinas de sobremesa de personalización de tarjetas de identificación, las siguientes cantidades y tipos:
97 x CLPS4 (68 siguen aún en servicio)
146 x CLP60
81 x CLP60-X

Estas máquinas han sido instaladas en Comisarías de Policía nacionales para los procesos de personalización de documentos de identidad.
Con esto confirmo una cooperación exitosa con Mühlbauer que nos ha apoyado en todos los asuntos de una manera flexible y orientada al cliente.

José Miguel Fernández de Liencres.
Director Comercial de la FNMT-RCM, E.P.E., M.P

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

Die Ablichtung stimmt mit der Urschrift überein.
Roding, 10. SEP. 2024

Notarin
Notar a. H. Klaus Ziegler
als Vertr. Bestellter Vertreter
der Notarin Katharina Gardner

NOTARIN KATHARINA MARCHNER RODING

C/ Jorge Juan, 106 [28009 Madrid]
Teléfono: +34 915 666 551
jmliencres@fnmt.es

851

Gz. 91 E 297/2024

Die Echtheit vorstehender Unterschrift des amtlich bestellten
Vertreters der Notarin Katharina Marchner in Roding

Notar außer Dienst Klaus Ziegler

und die Echtheit des beigedrückten Dienstsiegels
werden hiermit bestätigt.

Zugleich wird bescheinigt, dass der/die Vorgenannte
zur Vornahme der Amtshandlung gesetzlich befugt war.

Regensburg, den 12. September 2024

Der Präsident des Landgerichts
Im Auftrag

Wanner Manuela
Justizangestellte

BAYERN LANDGERICHT REGENSBURG

Kostenrechnung
Gebühr: 25,00 €
(gem. Art. 1 Abs. 1 LJKostG, LV.m.
§ 4 Abs. 1 JVKostG, KV 13.10

Consulado General de la República Dominicana
en Frankfurt, Alemania

Certifica: Visto bueno para legalizar la firma y el sello de WANNER MANUELA , PRESIDENTE DE LA AUDIENCIA PROVINCIAL, DE LA CIUDAD DE REGENSBURG, ALEMANIA., por ser, al parecer, auténtica sin prejuzgar la veracidad del contenido del documento ni ulterior destino que pueda darsele. Dado en FRANKFURT AM MAIN, ALEMANIA . El día 13 del mes de Febrero del año 2025.

Nicole Marie Espaillat Vega
Viceconsul

CONSORCIO EMDOC
EMDOC CONSORCIO
Santo Domingo

852

Experiencia en República Dominicana en proyectos de mantenimiento de tecnología en gobierno con al menos cinco (5) años de experiencia

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

853

GOBIERNO DE LA
REPÚBLICA DOMINICANA

HACIENDA

20 de febrero 2025

Señores,
Comité de Compras y Contrataciones,
Junta Central Electoral (JCE)
Santo Domingo, República de Dominicana

Proceso de Ref.: **JCE-CCC-LPI-2024-0001**

Estimados Señores:

Por este medio certificamos que, la empresa **IQTEK Solutions S.R.L.** participó y resultó ganadora en varios procesos de compras en proyectos de soporte y mantenimiento, de esta institución en el año 2020 y 2021, entre los cuales se encuentran los siguientes:

1. Renovación de soporte y mantenimiento Central Telefónica del Ministerio de Hacienda, Referencia Nm: MH-CCC-CP-2020-0007.

2. Solicitud de renovación de soporte y mantenimiento soluciones informáticas del Ministerio de Hacienda, Referencia Núm: MH-CCC-CP-2020-0003, lote II.

3. Lote III y VI del "procedimiento de licitación Pública Nacional para la "Renovación y mantenimiento de soluciones informáticas del Ministerio de Hacienda, Referencia Núm: HM-CCC-LPN-2021-0005".

Ref: JCE-CCC-LPI-2024-0001 «Contratación de la empresa que se encargará de suplir los equipos, materiales y servicios para la impresión de la nueva Cédula de Identidad y Electoral (CIE) y Cédula de Identidad (CI)».

Atentamente,

Sandy Santos
Encargado de Operaciones TIC

GOBIERNO DE LA MINISTERIO DE HACIENDA Dirección de Investigación de la Información y Comunicación VICEMINISTERIO TÉCNICO ADMINISTRATIVO REPÚBLICA DOMINICANA

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

854

REPÚBLICA DOMINICANA
HACIENDA

Contrato de Ejecución de Servicios núm. MH-2021-000003

Celebrado entre:

EL MINISTERIO DE HACIENDA

y

IQTEK SOLUTIONS, S. R. L.

«Renovación de soporte y mantenimiento Central Telefónica del Ministerio de Hacienda, Referencia núm. MH-CCC-CP-2020-0007

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

855

CONTRATO DE EJECUCIÓN DE SERVICIOS

ENTRE:

De una parte, **EL MINISTERIO DE HACIENDA**, institución del Estado dominicano, organizado y establecido de conformidad con la Ley núm. 494-06, ubicado en la avenida México núm. 45, sector Gascue, Santo Domingo de Guzmán, Distrito Nacional, capital de la República Dominicana, debidamente representado por el señor **FRIXO MESSINA ARVELO**, Viceministro Técnico Administrativo, dominicano, mayor de edad, titular de la cédula de identidad y electoral núm. 001-0130166-1, con domicilio en esta ciudad de Santo Domingo de Guzmán, Distrito Nacional, capital de la República Dominicana, quien actúa en virtud de la Resolución núm. 195-2020 de fecha diecinueve (19) de agosto de dos mil veinte (2020), emitida por este Ministerio, quien en lo adelante se denominará como «**LA ENTIDAD CONTRATANTE**», o por su nombre completo; y

De la otra parte, la sociedad comercial **IQTEK SOLUTIONS, S. R. L.**, constituida de conformidad con la leyes de la República Dominicana, provista del Registro Nacional de Contribuyente (R. N. C.) núm. 1-30-87696-7, con su domicilio social situado en la calle Galá núm. 8, sector Arroyo Hondo Viejo, Santo Domingo de Guzmán, Distrito Nacional, capital de la República Dominicana, debidamente representada por el señor **FRANKLIN GEOVANNY CIPRIÁN GOODIN**, dominicano, mayor de edad, titular de la cédula de identidad núm. 001-0908680-1, domiciliado y residente en esta ciudad de Santo Domingo de Guzmán, Distrito Nacional, capital de la República Dominicana, quien actúa en virtud del Acta de Asamblea General Extraordinaria de fecha trece (13) de enero de dos mil veinte (2020), quien para los fines del presente contrato, se denominará "**LA PRESTADORA DE SERVICIO**", o por su nombre completo.

Para referirse a ambos se les denominará **LAS PARTES.**

PREÁMBULO

POR CUANTO: que la Ley núm. 340-06, de fecha dieciocho (18) de agosto de dos mil seis (2006), sobre Compras y Contrataciones Públicas de Bienes, Servicios, Obras y Concesiones, y su posterior modificación contenida en la Ley núm. 449-06, de fecha seis (6) de diciembre de dos mil seis (2006), establece entre los Procedimientos de Selección por Comparación de Precios.

POR CUANTO: que la referida Ley, en su artículo 16, numeral 4, establece que:«Comparación de Precios es una amplia convocatoria a las personas naturales o jurídicas inscritas en el registro respectivo. Este proceso sólo aplica para la compra de bienes comunes con especificaciones estándares, adquisición de servicios y obras menores. Un procedimiento simplificado, establecido por un reglamento de la presente ley, será aplicable al caso de compras menores».

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo

356

POR CUANTO: que el artículo 17 de la referida Ley, establece la tabla contentiva de los factores mediante la cual se determina los umbrales topes que sirven de base para la selección del Procedimiento a aplicar en un proceso de compra o contratación.

POR CUANTO: que la Resolución núm. PNP-01-2020, de fecha siete (7) de enero del año dos mil veinte (2020), emitida por la Dirección General de Contrataciones Públicas (DGCP), fija los umbrales para la determinación de los Procedimientos de Selección a utilizar en la contratación de bienes, servicios y obras, durante el ejercicio correspondiente al año dos mil veinte (2020).

POR CUANTO: que mediante el Acto Administrativo núm. 064-2020, de fecha dieciocho (18) de noviembre de dos mil veinte (2020), el Comité de Compras y Contrataciones de este Ministerio, autorizó el Procedimiento de Comparación de Precios, aprobó la Ficha Técnica/Términos de Referencia y designó los peritos técnicos para la «Renovación de soporte y mantenimiento Central Telefónica del Ministerio de Hacienda, Referencia núm. MH-CCC-CP-2020-0007».

POR CUANTO: que después de un minucioso estudio de las propuestas técnicas «Sobres A» y económicas «Sobres B» presentadas por los oferentes participantes, el Comité de Compras y Contrataciones de este Ministerio de Hacienda, mediante el Acto Administrativo núm. 071-2020, de fecha veintiuno (21) de diciembre de dos mil veinte (2020), adjudicó al oferente **IQTEK SOLUTIONS, S. R. L.**, el Procedimiento de Comparación de Precios de Referencia núm. MH-CCC-CP-2020-0007.

POR CUANTO: que **LA ENTIDAD CONTRATANTE** procedió a la notificación de los resultados finales del citado procedimiento.

POR CUANTO: que en fecha catorce (14) de enero de dos mil veintiuno (2021), **LA PRESTADORA DE SERVICIO** constituyó la Garantía de Fiel Cumplimiento de Contrato, Fianza núm. 1-Ffc-5600, con la entidad Compañía Dominicana de Seguros, S. R. L., correspondiente al cuatro por ciento (4%) del monto total adjudicado, en cumplimiento a las disposiciones del artículo 112, del Decreto núm. 543-12, de fecha seis (6) de septiembre de dos mil doce (2012) contentivo del Reglamento de Aplicación de la Ley núm. 340-06 y sus modificaciones.

POR LO TANTO, y en el entendido de que el anterior preámbulo forma parte integral del presente Contrato.

LAS PARTES HAN CONVENIDO Y PACTADO LO SIGUIENTE:

ARTÍCULO 1: DEFINICIONES:

Siempre que en el presente Contrato se empleen los siguientes términos, se entenderá que significan lo que expresa a continuación:

a) **Contrato**: el presente documento.

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo

857

b) **Coordinador**: la persona física que actúa en nombre y representación de **LA ENTIDAD CONTRATANTE** para la coordinación de los servicios.
c) **La Prestadora de Servicio:** nombre de la persona natural o jurídica, consorcio, que ejecutará el objeto del Contrato.
d) **Entidad Contratante**: **EL MINISTERIO DE HACIENDA**.
e) **Máxima Autoridad Ejecutiva**: el titular o representante legal de **EL MINISTERIO DE HACIENDA**.
f) **Monto del Contrato**: el importe señalado en el contrato.
g) **Oferente/Proponente:** persona natural o jurídica que presenta credenciales a los fines de participar en un procedimiento de contratación.

ARTÍCULO 2.- DOCUMENTOS CONSTITUYENTES DEL CONTRATO

Los siguientes documentos forman parte integral e insustituible del presente Contrato, y **LA PRESTADORA DE SERVICIO** reconoce cada uno de estos como parte intrínseca del mismo:

a) El Contrato.
b) La Ficha Técnica/Términos de Referencia del procedimiento.
c) La Oferta Técnica «Sobre A» y la Oferta Económica «Sobre B» de **LA PRESTADORA DE SERVICIO**.
d) Documentos de **LA PRESTADORA DE SERVICIO**.
e) Garantía de Fiel Cumplimiento del Contrato.

ARTÍCULO 3.- OBJETO DEL CONTRATO.

LA PRESTADORA DE SERVICIO, por medio del presente Contrato se compromete a cumplir con todos los requisitos establecidos en la Ficha Técnica/Términos de Referencia del Procedimiento de Comparación de Precios para la «Renovación de soporte y mantenimiento central telefónica del Ministerio de Hacienda, Referencia núm. MH-CCC- CP-2020-0007».

ARTÍCULO 4.- MONTO DEL CONTRATO.

El monto total convenido por la prestación de servicios objeto del presente Contrato, asciende a la suma de **OCHOCIENTOS MIL CUATROCIENTOS VEINTIDÓS PESOS DOMINICANOS CON 03/100 (RD$800,422.03)**, este monto incluye Impuesto sobre Transferencia de Bienes Industrializados y Servicios (ITBIS).

ARTICULO 5. - FORMA DE PAGO.

5.1 El pago será realizado en pesos dominicanos.

5.2 La **ENTIDAD CONTRATANTE** establece la siguiente modalidad de pago, a saber: crédito a sesenta (60) días luego de la entrega de certificación de renovación de soporte y mantenimiento.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

ARTÍCULO 6.- TIEMPO DE VIGENCIA.

El presente contrato tendrá una vigencia de un (1) año, contado a partir del día veinte (20) de enero de dos mil veintiuno (2021) hasta el día veinte (20) de enero de dos mil veintidós (2022) o hasta la recepción conforme de los servicios objeto del presente Contrato.

ARTÍCULO 7.- NO RELACIÓN LABORAL.

LAS PARTES aceptan y reconocen que el presente Contrato no establece una relación de subordinación laboral entre ellas bajo el Código de Trabajo de la República Dominicana.

LAS PARTES acuerdan, por este medio, liberarse mutuamente de toda acción o demanda laboral que ella o su personal, sus empleados y / o representantes intentaren en su contra, derivada del cumplimiento y ejecución del presente Contrato.

ARTÍCULO 8.- FUERZA MAYOR Y CASO FORTUITO.

8.1 Ni **LA ENTIDAD CONTRATANTE** ni **LA PRESTADORA DE SERVICIO** serán responsables de cualquier incumplimiento de El Contrato si su ejecución ha sido demorada, impedida, obstaculizada o frustrada por causas de Fuerza Mayor o Caso Fortuito.

8.2 Para los efectos del presente Contrato, Fuerza Mayor significa cualquier evento o situación que escapen al control de una parte, imprevisible e inevitable, y sin que esté envuelta su negligencia o falta, como son, a manera enunciativa pero no limitativa, actos de autoridades gubernamentales o militares, regulaciones o requerimientos gubernamentales, epidemias, guerras, actos de terroristas, huelgas, fuegos, explosiones, temblores de tierra, accidentes, catástrofes, inundaciones y otras perturbaciones ambientales mayores, condiciones severas e inusuales del tiempo.

8.3 Caso Fortuito significa aquel acontecimiento que no ha podido preverse, o que previsto no ha podido evitarse, por ser extraño a la voluntad de las personas.

8.4 Las causas de Fuerza Mayor o Caso Fortuito especificadas anteriormente no incluyen:

a) Cualquier evento causado por negligencia o acción intencional de una parte.
b) Cualquier evento que una de las partes pudo haber tomado en cuenta al momento de la firma o de la ejecución de este Contrato para evitar incumplimiento de sus obligaciones.
c) Insuficiencia de recursos o fallas en el cumplimiento de cualquier pago bajo este Contrato.

8.5 La falla de una parte involucrada en el presente Contrato, que le impida

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

859

cumplir cualquiera de sus obligaciones, no será considerada como incumplimiento, siempre y cuando éste surja de un evento de Fuerza Mayor o Caso Fortuito y la parte afectada haya tomado todas las precauciones razonables, con el debido esmero y cuidado, siempre con el objetivo de cumplir con los términos y condiciones establecidos en este Contrato.

8.6 Si por una causa de Fuerza Mayor o Caso Fortuito, **LA PRESTADORA DE SERVICIO** no concluye sus labores en el plazo establecido, **LA ENTIDAD CONTRATANTE** extenderá el Contrato por un tiempo igual al período en el cual **LA PRESTADORA DE SERVICIO** no pudo cumplir, debido únicamente a esta causa.

8.7 **LA PRESTADORA DE SERVICIO** tendrá derecho al pago o los pagos establecidos en el presente Contrato durante el período de incumplimiento como resultado de una causa de Fuerza Mayor o Caso Fortuito. Igualmente tendrá derecho al reembolso de cualquier gasto adicional directamente relacionado con las obligaciones resultantes del Contrato en el que incurra durante el período de Fuerza Mayor o Caso Fortuito.

8.8 Si **LA PRESTADORA DE SERVICIO** dejara de presentar tal reclamación o de dar el aviso requerido dentro del periodo especificado, se considerará como que ha renunciado a su derecho en relación a la ocurrencia de la Fuerza Mayor o Caso Fortuito.

ARTÍCULO 9.- MEDIDAS A TOMAR.

LAS PARTES acuerdan que:

a) La parte afectada por un evento de Fuerza Mayor o Caso Fortuito deberá tomar las medidas razonables para suprimir la inhabilidad de la otra Parte en cumplir con sus obligaciones.

b) La parte afectada por un evento de Fuerza Mayor o Caso Fortuito deberá notificar, en un plazo no mayor de veinticuatro (24) horas y por escrito a la otra parte la ocurrencia del evento, indicando su naturaleza y causa; de igual manera deberá notificar por escrito a la otra parte la restauración de las condiciones normales tan pronto se resuelva la situación de Fuerza Mayor o Caso Fortuito.

c) Las partes adoptarán todas las medidas posibles para reducir las consecuencias adversas de un evento de Fuerza Mayor o Caso Fortuito.

ARTÍCULO 10.- OBLIGACIONES DE LA PRESTADORA DE SERVICIO.

10.1 LA PRESTADORA DE SERVICIO prestará los servicios previstos en el presente Contrato como se describen en el Pliego de Condiciones Específicas.

10.2 LA PRESTADORA DE SERVICIO presentará a **LA ENTIDAD CONTRATANTE**, de su propia iniciativa o a solicitud de aquella, todas las informaciones y aclaraciones relacionadas con la ejecución del Contrato.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

860

10.3 **LA PRESTADORA DE SERVICIO** realizará los servicios y cumplirá sus obligaciones establecidas bajo este Contrato con diligencia, eficiencia y economía, conforme a las normas y prácticas generalmente aceptadas y a las normas para el ejercicio del servicio contratado, reconocidas por los organismos internacionales y nacionales. Asimismo, empleará métodos ortodoxos de administración y utilizará la tecnología avanzada más adecuada, así como los equipos, maquinarias y materiales más seguros y eficaces durante el desempeño de su gestión.

10.4 **LA PRESTADORA DE SERVICIO** ejecutará y concluirá sus servicios y subsanará cualquier deficiencia en los mismos identificadas por **LA ENTIDAD CONTRATANTE** con el cuidado y la diligencia debidos y en riguroso cumplimiento de las disposiciones del Contrato.

10.5 **LA PRESTADORA DE SERVICIO** se atendrá a las órdenes administrativas impartidas por **LA ENTIDAD CONTRATANTE**. Cuando **LA PRESTADORA DE SERVICIO** considere que las exigencias de una orden administrativa sobrepasan El Contrato, deberá notificarlo a **LA ENTIDAD CONTRATANTE** en un plazo de quince (15) días a partir del recibo de la orden administrativa. La ejecución de la orden administrativa no se suspenderá como consecuencia de dicha notificación.

10.6 **LA PRESTADORA DE SERVICIO** respetará y cumplirá toda la legislación y normativa vigente en el Estado dominicano.

ARTÍCULO 11.- CONFLICTO DE INTERESES.

LA PRESTADORA DE SERVICIO no se beneficiará de otros pagos. El pago a ser recibido por **LA PRESTADORA DE SERVICIO,** previsto en el artículo 4 del presente Contrato, constituye la única remuneración con relación al alcance del mismo. Por tanto, **LA PRESTADORA DE SERVICIO** no podrá exigir ningún pago adicional por ningún concepto en relación con las actividades establecidas en este Contrato o en cumplimiento de sus obligaciones. Además, **LA PRESTADORA DE SERVICIO** utilizará sus mejores esfuerzos para asegurar que su personal técnico tampoco reciba remuneración adicional a la prevista en este Contrato.

ARTÍCULO 12.- PROHIBICIÓN DE ACTIVIDADES CONFLICTIVAS.

Ni **LA PRESTADORA DE SERVICIO** ni su personal técnico acreditado tendrán derecho a comprometerse, directa o indirectamente, en cualquier negocio o actividad profesional que pueda producir un conflicto de intereses con las responsabilidades puestas a su cargo en virtud de este Contrato.

ARTÍCULO 13.- CONFIDENCIALIDAD.

Todos los informes y documentos que se produzcan como consecuencia del presente Contrato no podrán ser divulgados a terceras personas o instituciones, durante ni después de la expiración del presente Contrato, sin la autorización escrita de **LAS PARTES.**

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

861

ARTÍCULO 14.- GARANTÍA DE FIEL CUMPLIMIENTO DE CONTRATO.

Para garantizar el fiel cumplimiento del presente contrato, **LA PRESTADORA DE SERVICIO**, en fecha catorce (14) de enero de dos mil veintiuno (2021), hace formal entrega de la Fianza núm. 1-Ffc-5600, expedida por Compañía Dominicana de Seguros, S. R. L., a favor de **LA ENTIDAD CONTRATANTE**, en cumplimiento con lo establecido en el artículo 112 del Reglamento de Aplicación de la Ley núm. 340-06 y sus modificaciones, aprobado mediante Decreto núm. 543-12.

PÁRRAFO I. La garantía del fiel cumplimiento de contrato responderá por los daños y perjuicios que experimente **EL MINISTERIO DE HACIENDA** en caso de incumplimiento por parte de **IQTEK SOLUTIONS, S. R. L.,** de las disposiciones contenidas en este contrato, toda vez que el mismo no sea por una causa justificada, notificada oportunamente a **LA ENTIDAD CONTRATANTE** o por causa de fuerza mayor. De comprobarse el incumplimiento, **EL MINISTERIO DE HACIENDA** procederá a ejecutar la garantía, independientemente de las acciones judiciales que correspondan.

PÁRRAFO II. La garantía solicitada ha sido expedida por una compañía de seguro del mercado dominicano, Compañía Dominicana de Seguros, S. R. L., de acuerdo a la última publicación realizada por la Superintendencia de Seguros.

PÁRRAFO III. En caso de que a la llegada del término de la vigencia de esta garantía se continúe prestando los servicios objeto de este contrato **IQTEK SOLUTIONS, S. R. L.**, queda obligada a renovarla automáticamente por el período que fuera acordado entre **LAS PARTES.**

PÁRRAFO IV. Dicha garantía responderá de los daños y perjuicios que se produzcan a **LA ENTIDAD CONTRATANTE** en caso de incumplimiento, que determinará en todo caso la ejecución de la Garantía, independientemente del resto de acciones que legalmente proceden.

ARTÍCULO 15.- INDEMNIZACIÓN POR PARTE DE LA PRESTADORA DE SERVICIO.

LA PRESTADORA DE SERVICIO será responsable dentro de los límites de su seguro de responsabilidad civil general, de indemnizar a **LA ENTIDAD CONTRATANTE** total y efectivamente contra toda pérdida, daños, perjuicios, muertes, gastos, acción, procedimiento, demanda, costos y reclamaciones de una tercera persona, ocurrida durante la vigencia del presente Contrato, incluyendo, pero sin limitar, a honorarios y

gastos legales incurridos por **LA ENTIDAD CONTRATANTE,** pero solamente en la medida en que tales pérdidas, daños, o perjuicios sean resultado de actos ilícitos o negligencia de **LA PRESTADORA DE SERVICIO,** así como del uso o violación de cualquier patente de invención o propiedad intelectual o de cualquier hecho o acontecimiento que resulte como consecuencia de su falta

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.

862

ARTÍCULO 16.- OBLIGACIONES DE LA ENTIDAD CONTRATANTE.

LA ENTIDAD CONTRATANTE hará sus mejores esfuerzos para asegurar que:

a) Provea a **LA PRESTADORA DE SERVICIO** y a su personal técnico acreditado de cualquier documento gubernamental necesario para la realización de los servicios establecidos en este Contrato.

b) Emita las instrucciones necesarias a los agentes, funcionarios y representantes del Estado para la rápida y efectiva ejecución de los servicios.

ARTÍCULO 17.- EQUILIBRIO ECONÓMICO.

Si en fecha posterior a la entrada en vigencia del presente Contrato se producen cambios en las leyes nacionales, relativos y/o relacionados con la moneda nacional, que impliquen aumentos en el costo o en los gastos a incurrir por **LA PRESTADORA DE SERVICIO** para la realización de sus servicios, los pagos y los gastos reembolsables pagables a **LA PRESTADORA DE SERVICIO** en virtud de este Contrato aumentarán en la proporción correspondiente a las modificaciones que haya sufrido la legislación con relación a la devaluación de la moneda nacional.

ARTÍCULO 18.- MODIFICACIONES AL CONTRATO.

Cualquier modificación a los términos y condiciones del presente Contrato deberá hacerse por acuerdo mutuo entre **LAS PARTES**, por escrito, mediante enmiendas numeradas cronológicamente y la fecha de vigencia de cada una se contará a partir de la fecha de aprobación realizada por **LA ENTIDAD CONTRATANTE**.

ARTÍCULO 19.- SUSPENSIÓN.

19.1 Por parte de **LA ENTIDAD CONTRATANTE**:

19.1.2 LA ENTIDAD CONTRATANTE tendrá derecho a suspender los pagos e inclusive sus servicios a **LA PRESTADORA DE SERVICIO** mediante notificación escrita si **LA PRESTADORA DE SERVICIO** incumple sus obligaciones establecidas bajo este Contrato, siempre y cuando la notificación de la suspensión:

a) Especifique la naturaleza del incumplimiento, y
b) Requiera que **LA PRESTADORA DE SERVICIO** resuelva el incumplimiento dentro de un periodo no mayor de diez (10) días hábiles a partir del recibo de la notificación de suspensión.

19.2 Por parte de **LA PRESTADORA DE SERVICIO**:

19.2.1 LA PRESTADORA DE SERVICIO tendrá derecho a suspender la

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

prestación de sus servicios mediante notificación por escrito a **LA ENTIDAD CONTRATANTE**, si ésta incumple sus obligaciones establecidas en virtud de este Contrato, siempre y cuando la notificación de la suspensión:

a) Especifique la naturaleza del incumplimiento; y
b) Requiera que **LA ENTIDAD CONTRATANTE** resuelva el incumplimiento dentro de un periodo no mayor de diez (10) días hábiles a partir del recibo por parte de **LA ENTIDAD CONTRATANTE** de la notificación de suspensión.

19.3 La suspensión se aplicará a partir de la fecha de vencimiento del plazo indicado en la notificación.

ARTÍCULO 20.- RESCISIÓN DEL CONTRATO.

20.1 **LA ENTIDAD CONTRATATANTE** podrá rescindir el presente Contrato unilateralmente en el caso de falta grave de **LA PRESTADORA DE SERVICIO** y siempre que la misma no sea originada por acontecimientos de Fuerza Mayor o Caso Fortuito. En este caso, **LA ENTIDAD CONTRATATANTE** no compensará por ningún motivo a **LA PRESTADORA DE SERVICIO** por las sumas adeudadas.

20.2 **LA ENTIDAD CONTRATATANTE** podrá rescindir, sin responsabilidad ninguna, el presente Contrato, así como ejecutar la Fianza de Fiel Cumplimiento de Contrato, si **LA PRESTADORA DE SERVICIO** fuese a la quiebra, o si se extendiese contra él una orden de administración judicial, o si se presentase una petición de declaración en quiebra, o si hiciese algún convenio con sus acreedores o una cesión a favor de ellos.

20.3 En el caso en que **LA PRESTADORA DE SERVICIO** desee renunciar o que ambas partes deseen rescindir el Contrato por acuerdo mutuo, **LA ENTIDAD CONTRATATANTE compensará a LA PRESTADORA DE SERVICIO** de acuerdo al tiempo y al servicio suministrado objeto del presente contrato que haya sido ejecutado a la fecha.

ARTÍCULO 21.- CESE DE DERECHOS.

Con la rescisión del presente Contrato, conforme lo establecido en el artículo que antecede, cesan todos los derechos y obligaciones a excepción de:

a) Aquellos derechos y obligaciones de **LAS PARTES** que estén pendientes a la fecha de rescisión o terminación; y
b) La obligación de confidencialidad a que se refiere el artículo 21.

ARTÍCULO 22.- CESIÓN DE CONTRATO.

La capacidad técnica de **LA PRESTADORA DE SERVICIO** es el objetivo esencial de la utilización de sus servicios, por tanto, este Contrato no podrá ser cedido, ni en todo ni en parte. No obstante, **LA PRESTADORA DE SERVICIO** podrá utilizar los

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

servicios de otra firma asociada para el cumplimiento del mismo sin costo adicional para **LA ENTIDAD CONTRATATANTE.**

ARTÍCULO 23.- NULIDADES DEL CONTRATO.

La violación del régimen de prohibiciones establecido en el artículo 14 de la Ley núm. 340- 06 y sus modificaciones, originará la nulidad absoluta del Contrato, sin perjuicio de otra acción que decida interponer **LA ENTIDAD CONTRATATANTE.**

La división del presente Contrato, con el fin de evadir las obligaciones de la Ley núm. 340- 06 y sus modificaciones, y de las normas complementarias que se dicten en el marco del mismo, será causa de nulidad del mismo.

ARTÍCULO 24.- ARREGLO DE CONFLICTOS.

LAS PARTES se comprometen a realizar sus mejores esfuerzos para resolver en forma amigable los conflictos o desacuerdos que pudieran surgir con relación al desarrollo del presente Contrato y su interpretación.

ARTÍCULO 25.- SOLUCIÓN DE CONTROVERSIAS.

Todo litigio, controversia o reclamación resultante de este Contrato o relativo al mismo, su incumplimiento, su interpretación, su resolución o nulidad será sometido al Tribunal Contencioso, Tributario, Administrativo, instituido mediante la Ley núm. 13-07, de fecha cinco (5) de febrero del dos mil siete (2007).

ARTÍCULO 26.- INTERPRETACIÓN DEL CONTRATO.

El significado e interpretación de los términos y condiciones del presente Contrato se hará al amparo de las leyes de la República Dominicana.

ARTÍCULO 27.- IDIOMA OFICIAL.

El presente Contrato ha sido redactado en español, que será el idioma de control para todos los asuntos relacionados con el significado e interpretación de los términos y condiciones del presente documento.

ARTÍCULO 28.- TITULOS.

Los títulos no limitarán, alterarán o modificarán el significado de este Contrato.

ARTÍCULO 29.- LEGISLACIÓN APLICABLE.

LA PRESTADORA DE SERVICIO realizará sus servicios de conformidad con las leyes nacionales y tomará todas las medidas necesarias para asegurar que su personal técnico cumpla con las leyes vigentes en la República Dominicana.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

ARTÍCULO 30.- ELECCIÓN DE DOMICILIO.

Para todos los fines y consecuencias del presente Contrato, **LAS PARTES** eligen domicilio en las direcciones que figuran en la parte introductora del presente Contrato, en el cual recibirán válidamente todo tipo de correspondencia o notificación relativa al presente Contrato, su ejecución y terminación.

ARTÍCULO 31.- ACUERDO INTEGRO.

El presente Contrato y sus anexos contienen todas las estipulaciones y acuerdos convenidos entre **LAS PARTES**; en caso de ambigüedad, duda o desacuerdo sobre la interpretación del mismo y sus documentos anexos, prevalecerá su redacción. Asimismo, se establece que, si alguna de las disposiciones de este Contrato se declarara inválida, las demás no serán afectadas y permanecerán plenamente vigentes.

HECHO Y FIRMADO en la ciudad de Santo Domingo de Guzmán, Distrito Nacional, capital de la República Dominicana, a los veinte (20) días del mes de enero del año dos mil veintiuno (2021), en tres (3) originales del mismo tenor y efecto, uno para cada una de las partes y el otro para los fines legales correspondientes.

FRIXO MESSINA ARVELO
Actuando a nombre y representación de
EL MINISTERIO DE HACIENDA

FRANKLIN GEOVANNY CIPRIÁN GOODIN
Actuando en nombre y representación de
IQTEK SOLUTIONS, S. R. L.

DR. JOSE MIGUEL DE HERRERA BUENO ABOGADO NOTARIO PUBLICO COLEGIATURA 4622 SANTO DOMINGO, R.D.

Yo, José M. De Herrera, Abogado Notario Público de los del Número de Distrito Nacional, provisto de la matrícula núm. 4622, **CERTIFICO Y DOY FE** que las firmas de los señores **FRIXO MESSINA ARVELO** y **FRANKLIN GEOVANNY CIPRIÁN GOODIN**, fueron puestas en mi presencia libre y voluntariamente, quienes me declararon que esas firmas son las que usan en los documentos de sus vidas públicas y privadas, por lo que merecen entera fe y crédito. En la ciudad de Santo Domingo de Guzmán, Distrito Nacional, capital de la República Dominicana, a los veinte (20) días del mes de enero del año dos mil veintiuno (2021).

NOTARIO PÚBLICO

DR. JOSE MIGUEL DE HERRERA BUENO ABOGADO NOTARIO PUBLICO COLEGIATURA 4622 SANTO DOMINGO, R.D.

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

864

GOBIERNO DE LA
REPÚBLICA DOMINICANA
HACIENDA

Contrato de Compra de Bienes y Servicios Conexos núm. MH-2021-000029

Celebrado entre:

EL MINISTERIO DE HACIENDA

y

IQTEK SOLUTIONS, S. R. L.

«Lote III y IV del "Procedimiento de Licitación Pública Nacional para la "Renovación y mantenimiento de soluciones informáticas del Ministerio de Hacienda, Referencia núm. MH-CCC-LPN-2021-0005"»

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

867

CONTRATO DE SUMINISTRO DE BIENES Y SERVICIOS CONEXOS

ENTRE:

De una parte, **EL MINISTERIO DE HACIENDA**, órgano del Estado dominicano, organizado y establecido de conformidad con la Ley núm. 494-06, ubicado en la avenida México núm. 45, sector Gascue, Santo Domingo de Guzmán, Distrito Nacional, capital de la República Dominicana, debidamente representada por el señor **FRIXO MESSINA ARVELO**, Viceministro Técnico Administrativo, dominicano, mayor de edad, titular de la cédula de identidad y electoral núm. 001-0130166-1, con domicilio en esta ciudad de Santo Domingo de Guzmán, Distrito Nacional, capital de la República Dominicana, quien actúa en virtud de la Resolución núm. 195-2020 de fecha diecinueve (19) de agosto de dos mil veinte (2020), emitida por este Ministerio, quien en lo adelante se denominará como «**LA ENTIDAD CONTRATANTE**», o por su nombre completo; y

De la otra parte, la sociedad comercial **IQTEK SOLUTIONS, S. R. L.**, constituida de conformidad con la leyes de la República Dominicana, provista del Registro Nacional de Contribuyente (RNC) núm. 1-30-87696-7, con su domicilio social situado en la calle Gala núm. 8, sector Arroyo Hondo Viejo, Santo Domingo de Guzmán, Distrito Nacional, capital de la República Dominicana, debidamente representada por el señor **FRANKLYN GEOVANNY CIPRIAN GOODIN**, dominicano, mayor de edad, casado, titular de la cédula de identidad y electoral núm. 001-0908680-1, domiciliado y residente en esta ciudad de Santo Domingo de Guzmán, Distrito Nacional, capital de la República Dominicana, quien actúa en virtud del Acta de la Asamblea General Extraordinaria de fecha doce (12) de julio de dos mil veintiuno (2021), quien para los fines del presente contrato, se denominará «**EL PROVEEDOR**», o por su nombre completo.

Para referirse a ambos se les denominará **LAS PARTES.**

PREÁMBULO

POR CUANTO: que la Ley núm. 340-06, de fecha dieciocho (18) de agosto de dos mil seis (2006), sobre Compras y Contrataciones Públicas de Bienes, Servicios, Obras y Concesiones, y su posterior modificación contenida en la Ley núm. 449-06, de fecha seis (6) de diciembre de dos mil seis (2006), establece entre los Procedimientos de Selección la Licitación Pública Nacional.

POR CUANTO: que la referida Ley, en el numeral 1 del artículo 16, establece además que: «Licitación Pública: es el procedimiento administrativo mediante el cual las entidades del Estado realizan un llamado público abierto, convocando a los interesados para que formulen propuestas, entre los cuales seleccionará la más conveniente conforme a los pliegos de condiciones correspondiente».

CONSORCIO EMDOC, EMDOC CONSORCIO, Santo Domingo, R.D.

POR CUANTO: que la Resolución núm. PNP-01-2021, de fecha cinco (5) de enero de dos mil veintiuno (2021), emitida por la Dirección General de Contrataciones Públicas, indica los umbrales para la determinación de los procedimientos de compras y contrataciones durante el ejercicio correspondiente al año dos mil veintiunos (2021).

POR CUANTO: que en fecha trece (13) de octubre de dos mil veintiuno (2021), mediante el Acto Administrativo núm. 037-2021, este Comité de Compras y Contrataciones, autorizó el Procedimiento de Licitación Pública, aprobó el Pliego de Condiciones Específicas y las Especificaciones Técnicas, y designó a los peritos técnicos y los evaluadores de credenciales legales para la «Renovación y mantenimiento de soluciones informáticas del Ministerio de Hacienda, Referencia núm. MH-CCC-LPN-2021-0005».

POR CUANTO: que después de un minucioso estudio de las propuestas técnicas y económicas «Sobres A y B» presentadas por los oferentes participantes, el Comité de Compras y Contrataciones de este Ministerio de Hacienda, mediante el Acto Administrativo núm. 054-2021 de fecha quince (15) de diciembre de dos mil veintiuno (2021), adjudicó al oferente **IQTEK SOLUTIONS, S. R. L.**, los Lotes III y IV del Procedimiento de Licitación Pública Nacional para la «Renovación y mantenimiento de soluciones informáticas del Ministerio de Hacienda, Referencia núm. MH-CCC-LPN-2021-0005».

POR CUANTO: que, en ese sentido, en fecha veinte (20) de diciembre de dos mil veintiuno (2021), **LA ENTIDAD CONTRATANTE** procedió a la notificación de los resultados finales del citado procedimiento a los oferentes participantes.

POR CUANTO: que en fecha veinte (20) de diciembre de dos mil veintiuno (2021), EL **PROVEEDOR** constituyó la Garantía de Fiel Cumplimiento de Contrato, Fianza núm. 1-Ffc-8627 con la entidad Compañía Dominicana de Seguros, S. R. L., correspondiente al cuatro por ciento (4%) del monto total adjudicado, en cumplimiento a las disposiciones del artículo 112, del Decreto núm. 543-12, de fecha seis (6) de septiembre de dos mil doce (2012) contentivo del Reglamento de Aplicación de la Ley núm. 340-06 y sus modificaciones.

POR LO TANTO, y en el entendido de que el anterior preámbulo forma parte integral del presente contrato.

LAS PARTES HAN CONVENIDO Y PACTADO LO SIGUIENTE:

ARTÍCULO 1. DEFINICIONES.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

Siempre que en el presente contrato se empleen los siguientes términos, se entenderá que significan lo que expresa a continuación:

a) **Contrato**: el presente documento.
b) **Coordinador**: la persona física que actúa en nombre y representación de **LA ENTIDAD CONTRATANTE** para la coordinación del suministro de los bienes.
c) **Máxima Autoridad Ejecutiva**: el titular o representante legal de **EL MINISTERIO DE HACIENDA**.
d) **Entidad Contratante**: **EL MINISTERIO DE HACIENDA**.
e) **Monto del Contrato:** el importe señalado en el contrato.
f) **Oferente/Proponente:** persona natural o jurídica que presenta credenciales a los fines de participar en un procedimiento de contratación.
g) **Bienes:** productos elaborados a partir de materias primas, consumibles para el funcionamiento de los entes estatales.
h) **Proveedor:** Oferente/Proponente que, habiendo participado en el procedimiento de compra, resulta adjudicatario del contrato y suministra los bienes y servicios de acordados.

ARTÍCULO 2. DOCUMENTOS CONSTITUYENTES DEL CONTRATO.

Los siguientes documentos forman parte integral e insustituible del presente contrato, y **EL PROVEEDOR** reconoce cada uno de estos como parte intrínseca del mismo:

a) El contrato.
b) El Pliego de Condiciones Específicas y Especificaciones Técnicas.
c) La Oferta Técnica «Sobre A» y la Oferta Económica «Sobre B» de **EL PROVEEDOR**.
d) Documentos de **EL PROVEEDOR**; y
e) Garantía de Fiel Cumplimiento del Contrato.

ARTÍCULO 3. OBJETO DEL CONTRATO.

3.1 **EL PROVEEDOR** por medio del presente contrato se compromete a suministrar los bienes y servicios conexos detallados en el Pliego de Condiciones Específicas y las Especificaciones Técnicas correspondientes a los Lotes III y IV del Procedimiento de Licitación Pública Nacional para la «Renovación y mantenimiento de soluciones informáticas del Ministerio de Hacienda, Referencia núm. MH-CCC-LPN-2021-0005», detallados a continuación:

3.1.1 Lote III:
a) Renovación HPE Foundation Care
b) Renovación HP Proactive Care Advanced
c) Renovación Basic Support subscription Vmware

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

870

3.1.2 Lote IV: Renovación Soporte y Mantenimiento Netapp.

3.2 Asimismo, se compromete a cumplir con todo lo presentado en sus propuestas técnicas y económicas.

3.3 Los bienes y servicios conexos que integran el objeto del presente contrato deberán reunir los requisitos de calidad y presentación establecidos en el Pliego de Condiciones Específicas y las Especificaciones Técnicas.

3.4 **EL PROVEEDOR** deberá entregar la cantidad de bienes y servicios conexos requeridos de conformidad con lo establecido en Pliego de Condiciones Específicas y las Especificaciones Técnicas.

ARTÍCULO 4. MONTO DEL CONTRATO.

LAS PARTES convienen que el total monto a pagar por los bienes y servicios conexos objeto de este contrato, asciende a la suma de **once millones doscientos treinta y ocho mil seiscientos veintinueve pesos dominicanos con 33/100 (RD$11,238,629.33)**, este monto incluye Impuesto sobre Transferencia de Bienes Industrializados y Servicios (ITBIS), conforme se detalla a continuación:

A) El monto de seis millones ciento veintisiete mil ciento setenta y nueve pesos dominicanos con 31/00 (RD$6,127,179.31), correspondiente al Lote III.

B) El monto de cinco millones ciento once mil cuatrocientos cincuenta pesos dominicanos con 02/100 (RD$5,111,450.02), correspondiente al Lote IV.

ARTÍCULO 5. FORMA DE PAGO.

5.1 El pago será realizado en pesos dominicanos.

5.2 La **ENTIDAD CONTRATANTE** procederá a realizar un (1) único pago correspondiente al cien por ciento (100%), este se realizará con entrega total y recepción conforme de los bienes y servicios requeridos.

5.3 **EL PROVEEDOR** no estará exento del pago de los impuestos que pudieren generarse en virtud del presente contrato.

ARTÍCULO 6. TIEMPO DE VIGENCIA.

CONSORCIO EMDOC
EMDOC CONSORCIO
Santo Domingo, R.D.

El presente contrato de Suministro de Bienes y Servicios Conexos tendrá una vigencia de un (1) año, contados a partir del día veinte (20) de diciembre del año dos mil veintiuno (2021) hasta el día veinte (20) de diciembre del año dos mil veintidós (2022).

ARTÍCULO 7. OBLIGACIONES DE EL PROVEEDOR.

7.1 **EL PROVEEDOR** suministrará los bienes y servicios conexos previstos en el presente contrato como se describen en el Pliego de Condiciones Específicas y las Especificaciones Técnicas del procedimiento Referencia núm. MH-CCC-LPN-2021-0005 y sus propuestas técnica y económica, cumpliendo con los tiempos y cronogramas establecidos.

7.2 **EL PROVEEDOR** presentará a **LA ENTIDAD CONTRATANTE**, de su propia iniciativa o a solicitud de aquella, todas las informaciones y aclaraciones relacionadas con la ejecución del contrato.

7.3 **EL PROVEEDOR** suministrará los bienes y servicios conexos cumpliendo con sus obligaciones establecidas bajo este contrato con diligencia, eficiencia y economía, conforme a las normas y prácticas generalmente aceptadas y a las normas para el suministro de los bienes y servicios conexos contratado, reconocidas por los organismos internacionales y nacionales. Asimismo, empleará técnicas y métodos ortodoxos de administración y utilizará la tecnología avanzada más adecuada, así como los equipos, maquinarias y materiales más seguros y eficaces durante el desempeño de su gestión.

7.4 **EL PROVEEDOR** actuará en todo momento como asesor fiel con relación a cualquier asunto relacionado con sus servicios o con este contrato y apoyará y resguardará los intereses de **LA ENTIDAD CONTRATANTE** cuando esté tratando con otros contratistas o terceras personas.

7.5 **EL PROVEEDOR** ejecutará y concluirá sus servicios y subsanará cualquier deficiencia en los mismos identificadas por **LA ENTIDAD CONTRATANTE** con el cuidado y la diligencia debidos y en riguroso cumplimiento de las disposiciones del contrato.

7.6 **EL PROVEEDOR** se atendrá a las órdenes administrativas impartidas por **LA ENTIDAD CONTRATANTE**. Cuando **EL PROVEEDOR** considere que las exigencias de una orden administrativa sobrepasan el contrato, deberá notificarlo a **LA ENTIDAD CONTRATANTE** en un plazo de diez (10) días a partir del recibo de la orden administrativa. La ejecución de la orden administrativa no se suspenderá como consecuencia de dicha notificación.

7.7 **EL PROVEEDOR** respetará y cumplirá toda la legislación y normativa vigente en el Estado dominicano.

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo R.D.

7.8 **EL PROVEEDOR** deberá de emplear únicamente técnicos competentes y experimentados en sus especialidades respectivas, así como personal y jefes de equipos capaces para garantizar la debida ejecución del servicio, de conformidad con lo establecido en el Pliego de Condiciones Específicas, Especificaciones Técnicas y su oferta técnica.

7.9 Durante la ejecución del presente contrato, **EL PROVEEDOR** no deberá prescindir del personal profesional presentado en su propuesta técnica, no obstante, en caso de que por razones ajenas a la voluntad de **EL PROVEEDOR** sea necesario el reemplazo de cualquier persona esta se compromete a reemplazarlo por una persona con semejantes aptitudes y experiencia, el cual deberá contar con la aprobación de **LA ENTIDAD CONTRATANTE. LA ENTIDAD CONTRATANTE** se reserva el derecho de objetar cualquier personal, en cualquier momento, siempre y cuando existan causas justificadas para hacerlo.

ARTÍCULO 8. CONFLICTO DE INTERESES.

EL PROVEEDOR no se beneficiará de otros pagos. El pago a ser recibido por **EL PROVEEDOR** previsto en el artículo 4 del presente contrato, constituye la única remuneración con relación al alcance de este. Por tanto, **EL PROVEEDOR** no podrá exigir ningún pago adicional por ningún concepto en relación con las actividades establecidas en este contrato o en cumplimiento de sus obligaciones. Además, **EL PROVEEDOR** utilizará sus mejores esfuerzos para asegurar que su personal técnico tampoco reciba remuneración adicional a la prevista en este contrato.

ARTÍCULO 9. PROHIBICIÓN DE ACTIVIDADES CONFLICTIVAS.

Ni **EL PROVEEDOR** ni su personal técnico acreditado tendrán derecho a comprometerse, directa o indirectamente, en cualquier negocio o actividad profesional que pueda producir un conflicto de intereses con las responsabilidades puestas a su cargo en virtud de este contrato.

ARTÍCULO 10. INDEMNIZACIÓN POR PARTE DE EL PROVEEDOR

10.1 EL PROVEEDOR será responsable de indemnizar a **LA ENTIDAD CONTRATANTE** total y efectivamente contra toda pérdida, daños, perjuicios, muertes, gastos, acción, procedimiento, demanda, costos y reclamaciones de una tercera persona, ocurrida durante la vigencia del presente contrato, incluyendo, pero sin limitar, a honorarios y gastos legales incurridos por **LA ENTIDAD CONTRATANTE,** pero solamente en la medida en que tales pérdidas, daños, o perjuicios sean resultado de actos ilícitos o negligencia de **EL PROVEEDOR,** así como del uso o violación de cualquier patente de invención o propiedad intelectual o de cualquier hecho o acontecimiento que resulte como consecuencia de su falta

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

10.2 **EL PROVEEDOR** será en todo momento la única responsable y protegerá a **LA ENTIDAD CONTRATANTE** y a su representante frente a cualquier reclamación de terceros por concepto de indemnización por daños de cualquier naturaleza o lesiones corporales producidas como consecuencia de la ejecución del presente Contrato por **EL PROVEEDOR**, y su respectivo personal.

ARTÍCULO 11.- OBLIGACIONES DE LA ENTIDAD CONTRATANTE:

LA ENTIDAD CONTRATANTE hará sus mejores esfuerzos para asegurar que:
a) Provea a **EL PROVEEDOR** y a su personal técnico acreditado de cualquier documento gubernamental necesario para la realización de los servicios establecidos en este contrato.

b) Emita las instrucciones necesarias a los agentes, funcionarios y representantes del Estado para la rápida y efectiva ejecución de los servicios.

ARTÍCULO 12. NO RELACIÓN LABORAL.

LAS PARTES aceptan y reconocen que el presente contrato no establece una relación de subordinación laboral entre ellas bajo el Código de Trabajo de la República Dominicana. **EL PROVEEDOR** acuerda, por este medio, liberar a **LA ENTIDAD CONTRATANTE** de toda acción o demanda laboral que ella o su personal, sus empleados y representantes intentaren en su contra, derivada del cumplimiento y ejecución del presente contrato.

ARTÍCULO 13. CONFIDENCIALIDAD.

13.1 **EL PROVEEDOR** se compromete a guardar estricta confidencialidad sobre toda la información que suministre **LA ENTIDAD CONTRATANTE**, o que lleguen a conocer sus empleados, contratistas, asesores, agentes y subcontratistas, si los hubiere, de manera verbal o por medio escrito, audiovisual, magnético, vía electrónica o por cualquier otro medio, en desarrollo del contrato, (en adelante «Información Confidencial»). La obligación de reserva y confidencialidad de la Información Confidencial estará vigente después de la terminación del contrato.

13.2 La información confidencial no incluye: a) la información que sea de dominio público con anterioridad a la fecha en que hubiese sido suministrada o que se haya hecho pública lícitamente durante la vigencia del Contrato; b) la información que está en posesión o pueda ser independientemente adquirida o desarrollada por cualquiera de las Partes sin violar ninguna de sus obligaciones contractuales o legales; c) Información sobre la cual sea aprobada su divulgación por medio de autorización escrita y sólo hasta el límite de dicha autorización; d) Información que haya sido conocida a través de terceros sin que exista la

obligación de mantenerla bajo confidencialidad, a menos que se tenga pleno conocimiento que dichos terceros no están autorizados para revelar o divulgar dicha información.

13.3 **EL PROVEEDOR** deberá implementar, mantener y hacer cumplir las medidas de seguridad administrativas, técnicas y físicas apropiadas para garantizar la seguridad y confidencialidad de las informaciones obtenidas y/o suministradas por la otra parte, protegiéndolos contra el acceso no autorizado o la utilización indebida. Estas garantías no podrán ser inferiores a las aceptadas por la industria, incluyendo la elaboración e implementación de un plan de seguridad de la información, los controles y restricciones de acceso a la información, la protección de los sistemas (por ejemplo, protección de intrusos), medidas de seguridad física, cifrado de datos y claves con vencimientos periódicos, controles periódicos, jerarquías, y la formación a conciencia en seguridad del personal.

13.4 **EL PROVEEDOR** será responsable ante cualquier revelación, empleo o divulgación de cualquier porción de la Información Confidencial. En todo caso, se obliga tanto en la ejecución del presente contrato como una vez terminado, a implementar todas las políticas vigentes en materia de protección de la información confidencial de sus clientes tratándola con especial responsabilidad, control y protección. Toda la información confidencial que una parte suministre a la otra será utilizada solamente para los efectos descritos en este contrato.

13.5 **EL PROVEEDOR** se obliga a informar a la otra parte sobre cualquier sospecha de pérdida, fuga o ataque contra la información a los que ha accedido, recolectado y/o tratado en relación con los servicios contratados, aviso que deberá dar una vez que tenga conocimiento de tales eventualidades. La pérdida, fuga y ataque contra información implica asimismo la obligación de **EL PROVEEDOR** de dar el trámite al incidente de seguridad conforme las buenas prácticas de la industria en manejo de incidentes.

13.6 **EL PROVEEDOR** será responsable por cualquier perjuicio que se cause a la otra parte como consecuencia directa o indirecta del incumplimiento de cualquiera de las obligaciones que se desprenden de la presente cláusula.

13.7 Independientemente de las acciones a las que haya lugar por el incumplimiento de las obligaciones de este contrato, si **EL PROVEEDOR** extravía o revela información confidencial, dará aviso inmediato a la **ENTIDAD CONTRATANTE** y tomará todas las medidas razonables y necesarias para minimizar los resultados de pérdida de la información o divulgación de esta sin autorización.

13.8 **EL PROVEEDOR** deberá implementar medidas de seguridad organizativas, administrativas y humanas, tanto técnicas y físicas como informáticas, las cuales deberán garantizar que este tipo de información no será usada, comercializada, cedida, transferida y/o no será sometida a cualquier otro tratamiento contraria a fines del presente contrato.

EMDOC CONSORCIO Santo Domingo, R.D.

De manera especial se obliga a no tratar esta información para uso propio o de terceros o como herramientas de prospección para su propio beneficio o el de un tercero.

ARTÍCULO 14. GARANTÍA DE FIEL CUMPLIMIENTO DE CONTRATO.

14.1 Para garantizar el fiel cumplimiento del presente contrato, **EL PROVEEDOR**, en fecha veinte (20) de diciembre de dos mil veintiuno (2021) hace formal entrega de la Fianza núm. 1-Ffc-8627, expedida por Compañía Dominicana de Seguros, S. R. L., a favor de **LA ENTIDAD CONTRATANTE**, la cual fue depositada en cumplimiento a las disposiciones del artículo 112, del Decreto núm. 543-12, de fecha seis (6) de septiembre de dos mil doce (2012) contentivo del Reglamento de Aplicación de la Ley núm. 340-06 y sus modificaciones.

14.2 La garantía del fiel cumplimiento de contrato responderá por los daños y perjuicios que experimente **EL MINISTERIO DE HACIENDA** en caso de incumplimiento por parte de **EL PROVEEDOR**, de las disposiciones contenidas en este contrato, toda vez que el mismo no sea por una causa justificada, notificada oportunamente a **LA ENTIDAD CONTRATANTE** o por causa de fuerza mayor. De comprobarse el incumplimiento, **EL MINISTERIO DE HACIENDA** procederá a ejecutar la garantía, independientemente de las acciones judiciales que correspondan.

14.3 La garantía solicitada ha sido expedida por una compañía de seguro del mercado dominicano, Compañía Dominicana de Seguros, S. R. L.

14.4 En caso de que a la llegada del término de la vigencia de esta garantía se continúe prestando los servicios objeto de este contrato **EL PROVEEDOR**, queda obligada a renovarla automáticamente por el período que fuera acordado entre **LAS PARTES**. Dicha garantía responderá de los daños y perjuicios que se produzcan a **LA ENTIDAD CONTRATANTE** en caso de incumplimiento, que determinará en todo caso la ejecución de la Garantía, independientemente del resto de acciones que legalmente proceden.

ARTÍCULO 15 FUERZA MAYOR Y CASO FORTUITO.

15.1 Ni **LA ENTIDAD CONTRATANTE** ni **EL PROVEEDOR** serán responsables de cualquier incumplimiento del contrato si su ejecución ha sido demorada, impedida, obstaculizada o frustrada por causas de Fuerza Mayor o Caso Fortuito. Para los efectos del presente contrato, Fuerza Mayor significa cualquier evento o situación que escapen al control de una parte, imprevisible e inevitable, y sin que esté envuelta su negligencia o falta, como son, a manera enunciativa pero no limitativa, actos de autoridades gubernamentales o militares, regulaciones o requerimientos gubernamentales, epidemias, guerras, actos de terroristas, huelgas, fuegos, explosiones, temblores de tierra, accidentes,

CONSORCIO EMDOC, CONSORCIO EMDOC, Santo Domingo, R.D.

catástrofes, inundaciones y otras perturbaciones ambientales mayores, condiciones severas e inusuales del tiempo.

15.2 Caso Fortuito significa aquel acontecimiento que no ha podido preverse, o que previsto no ha podido evitarse, por ser extraño a la voluntad de las personas.

15.3 Las causas de Fuerza Mayor o Caso Fortuito especificadas anteriormente no incluyen:

1. Cualquier evento causado por negligencia o acción intencional de una parte.
2. Cualquier evento que una de las partes pudo haber tomado en cuenta al momento de la firma o de la ejecución de este contrato para evitar incumplimiento de sus obligaciones.
3. Insuficiencia de recursos o fallas en el cumplimiento de cualquier pago bajo este contrato.

15.4 La falla de una parte involucrada en el presente contrato, que le impida cumplir cualquiera de sus obligaciones, no será considerada como incumplimiento, siempre y cuando éste surja de un evento de Fuerza Mayor o Caso Fortuito y la parte afectada haya tomado todas las precauciones razonables, con el debido esmero y cuidado, siempre con el objetivo de cumplir con los términos y condiciones establecidos en este contrato.

15.5 Si por una causa de Fuerza Mayor o Caso Fortuito, **EL PROVEEDOR** no concluye sus labores en el plazo establecido, **EL PROVEEDOR** extenderá el contrato por un tiempo igual al período en el cual **EL PROVEEDOR** no pudo cumplir, debido únicamente a esta causa.

ARTÍCULO 16. MEDIDAS A TOMAR

LAS PARTES acuerdan que:

a) La parte afectada por un evento de Fuerza Mayor o Caso Fortuito deberá tomar las medidas razonables para suprimir la inhabilidad de la otra Parte en cumplir con sus obligaciones.
b) La parte afectada por un evento de Fuerza Mayor o Caso Fortuito deberá notificar, en un plazo no mayor de veinticuatro (24) horas y por escrito a la otra parte la ocurrencia del evento, indicando su naturaleza y causa; de igual manera deberá notificar por escrito a la otra parte la restauración de las condiciones normales tan pronto se resuelva la situación de Fuerza Mayor o Caso Fortuito.
c) Las partes adoptarán todas las medidas posibles para reducir las consecuencias adversas de un evento de Fuerza Mayor o Caso Fortuito.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

ARTÍCULO 17. EQUILIBRIO ECONÓMICO.

Si en fecha posterior a la entrada en vigencia del presente contrato se producen cambios en las leyes nacionales, relativos y/o relacionados con la moneda nacional, que impliquen aumentos en el costo o en los gastos a incurrir por para el suministro de los bienes y servicios, los pagos a **EL PROVEEDOR**, en virtud de este contrato, aumentarán en la proporción correspondiente a las modificaciones que haya sufrido la legislación con relación a la devaluación de la moneda nacional.

ARTÍCULO 18.-MODIFICACIONES DEL CONTRATO:

Cualquier modificación a los términos y condiciones del presente contrato deberá hacerse por mutuo acuerdo entre **LAS PARTES**, por escrito, mediante enmiendas numeradas cronológicamente y la fecha de vigencia de cada una se contará a partir de la fecha de aprobación realizada por **LA ENTIDAD CONTRATANTE**.

ARTÍCULO 19. SUSPENSIÓN.

19.1 **LA ENTIDAD CONTRATANTE** tendrá derecho a suspender el pago a **EL PROVEEDOR** mediante notificación escrita, si **EL PROVEEDOR** incumple sus obligaciones establecidas bajo este contrato, siempre y cuando la notificación de la suspensión especifique la naturaleza del incumplimiento y requiera que **EL PROVEEDOR** resuelva el incumplimiento dentro de un período no mayor de diez (10) días hábiles a partir del recibo de la notificación de suspensión.

19.2 **EL PROVEEDOR** tendrá derecho a suspender la prestación de sus servicios mediante notificación por escrito a **LA ENTIDAD CONTRATANTE**, si ésta incumple sus obligaciones establecidas en virtud de este contrato, siempre y cuando la notificación de la suspensión especifique la naturaleza del incumplimiento y requiera que **LA ENTIDAD CONTRATANTE** resuelva el incumplimiento dentro de un período no mayor de diez (10) días hábiles a partir del recibo por parte de **LA ENTIDAD CONTRATANTE** de la notificación de suspensión.

19.3 La suspensión se aplicará a partir de la fecha de vencimiento del plazo indicado en la notificación.

ARTÍCULO 20. CESIÓN DE CONTRATO.

La capacidad técnica de **EL PROVEEDOR** es el objetivo esencial de la utilización de sus servicios, por tanto, este contrato no podrá ser cedido, ni en todo ni en parte, sin la autorización previa por escrito de **LA ENTIDAD CONTRATANTE**.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

ARTÍCULO 21.-RESCISIÓN DEL CONTRATO.

21.1 **LA ENTIDAD CONTRATANTE** podrá rescindir el presente contrato unilateralmente y ejecutar la Garantía de Fiel Cumplimiento de Contrato en el caso de falta grave de **EL PROVEEDOR**, siempre que esta no sea originada por acontecimientos de Fuerza Mayor o Caso Fortuito. En este caso, **EL PROVEEDOR** no compensará por ningún motivo a por las sumas adeudadas.

21.2 **LA ENTIDAD CONTRATANTE** podrá rescindir, sin responsabilidad ninguna, el presente contrato, así como ejecutar la Fianza de Fiel Cumplimiento de contrato, si fuese a la quiebra, o si se extendiese contra él una orden de administración judicial, o si se presentase una petición de declaración en quiebra, o si hiciese algún convenio con sus acreedores o una cesión a favor de ellos.

21.3 En el caso en que **EL PROVEEDOR** desee renunciar o que ambas partes deseen rescindir el contrato por acuerdo mutuo, **LA ENTIDAD CONTRATANTE** compensará a **EL PROVEEDOR** de acuerdo con el tiempo y al servicio suministrado objeto del presente contrato que haya sido ejecutado a la fecha.

ARTÍCULO 22. CESE DE DERECHOS.

Con la rescisión del presente contrato, conforme lo establecido en el artículo que antecede, cesan todos los derechos y obligaciones a excepción de:

(i) Aquellos derechos y obligaciones de **LAS PARTES** que estén pendientes a la fecha de rescisión o terminación; y
(ii) La obligación de confidencialidad a que se refiere el artículo 13.

ARTÍCULO 23. NULIDADES DEL CONTRATO.

23.1 La violación del régimen de prohibiciones establecido en el artículo 14 de la Ley núm. 340-06, sobre Compras y Contrataciones Públicas de Bienes, Servicios, Obras y Concesiones, su modificatoria, originará la nulidad absoluta del contrato, sin perjuicio de otra acción que decida interponer **LA ENTIDAD CONTRATANTE**.

23.2 La división del presente contrato, con el fin de evadir las obligaciones de la Ley núm. 340-06 y de las normas complementarias que se dicten en el marco de este, será causa de nulidad de este.

ARTÍCULO 24. SOLUCIÓN DE CONTROVERSIA.

CONSORCIO EMDOC
EMDOC CONSORCIO
Santo Domingo, R.D.

24.1 **LAS PARTES** se comprometen a realizar sus mejores esfuerzos para resolver en forma amigable los conflictos o desacuerdos que pudieren surgir con relación al desarrollo del presente contrato y su interpretación, en un plazo no mayor a diez (10) días hábiles a partir del inicio de las negociaciones.

24.2 Todo litigio, controversia o reclamación resultante de este contrato o relativo al mismo, su incumplimiento, su interpretación, su resolución o nulidad será sometido al Tribunal Superior Administrativo.

ARTÍCULO 25. INTERPRETACIÓN DEL CONTRATO.

El significado e interpretación de los términos y condiciones del presente contrato se hará al amparo de las leyes de la República Dominicana, y de manera particular con las disposiciones de derecho administrativo aplicables.

ARTÍCULO 26. LEGISLACIÓN APLICABLE.

La ejecución del presente contrato se realizará de conformidad con las leyes NACIONALES vigentes en la República Dominicana. **EL OFERENTE** tomará todas las medidas necesarias para asegurar que su personal técnico cumpla con las leyes vigentes en la República Dominicana.

ARTÍCULO 27. IDIOMA OFICIAL.

El presente contrato ha sido redactado en español, que será el idioma de control para todos los asuntos relacionados con el significado e interpretación de los términos y condiciones del presente contrato.

ARTÍCULO 28. TÍTULOS.

Los títulos que siguen al número de los artículos en el presente contrato sólo tienen un propósito ilustrativo y no servirán como base para interpretar el artículo completo o alterar, modificar el significado de estos.

ARTÍCULO 29. ACUERDO ÍNTEGRO:

El presente contrato, y sus anexos, contienen todo las estipulaciones y acuerdos convenidos entre **LAS PARTES**; en caso de ambigüedad, duda o desacuerdo sobre la interpretación de este y sus documentos anexos, prevalecerá su redacción. Asimismo, se establece que, si alguna de las disposiciones de este contrato se declara inválida, las demás no serán afectadas y permanecerán plenamente vigentes.

EMDOC CONSORCIO Santo Domingo

ARTÍCULO 30. ELECCIÓN DE DOMICILIO:

Para todos los fines y consecuencias del presente contrato, **LAS PARTES** eligen domicilio en las direcciones que figuran en la parte introductora del presente contrato, en el cual recibirán válidamente todo tipo de correspondencia o notificación relativa al presente contrato, su ejecución y terminación.

HECHO Y FIRMADO en la ciudad de Santo Domingo de Guzmán, Distrito Nacional, capital de la República Dominicana, a los veinte (20) días del mes de diciembre del año dos mil veintiuno (2021), en tres (3) originales del mismo tenor y efecto, uno para cada una de las partes y el otro para los fines legales correspondientes.

MINISTERIO DE HACIENDA
Santo Domingo, Rep. Dom.

FRIXO MESSINA ARVELO
Actuando a nombre y representación de
EL MINISTERIO DE HACIENDA

IQtek Solutions, S.R.L.
RNC: 130876987
Santo Domingo, R.D.

FRANKLYN GEOVANNY CIPRIAN GOODIN
Actuando en nombre y representación de
IQTEK SOLUTIONS, S. R. L

DR. JOSE MIGUEL DE HERRERA BUENO
ABOGADO NOTARIO PÚBLICO
CÉDULA 4612
SANTO DOMINGO, R.D.

Dr. José M. de Herrera, Abogado Notario Público de los del número del Distrito Nacional, provisto de la matrícula núm. 4612, **CERTIFICO Y DOY FE**, que las firmas de los señores **FRIXO MESSINA ARVELO** y **FRANKLYN GEOVANNY CIPRIAN GOODIN**, fueron puestas en mi presencia libre y voluntariamente, quienes me declararon que esas firmas son las que usan en los documentos de sus vidas públicas y privadas, por lo que merecen entera fe y crédito. En la ciudad de Santo Domingo de Guzmán, Distrito Nacional, capital de la República Dominicana, a los veinte (20) días del mes de diciembre del año dos mil veintiuno (2021).

NOTARIO PÚBLICO

DR. JOSE MIGUEL DE HERRERA BUENO
ABOGADO NOTARIO PÚBLICO
CÉDULA 4612
SANTO DOMINGO, R.D.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

881

GOBIERNO DE LA
REPÚBLICA DOMINICANA

HACIENDA

Contrato de Ejecución de Servicios núm. MH-2021-000005

Celebrado entre:

EL MINISTERIO DE HACIENDA

y

IQTEK SOLUTIONS, S. R. L.

Lote II: Soporte y mantenimiento de HPE

«Solicitud de renovación de soporte y mantenimiento soluciones informáticas del Ministerio de Hacienda, Referencia núm. MH-CCC-LPN-2020-0003»

882

CONTRATO DE EJECUCIÓN DE SERVICIOS

ENTRE:

De una parte, **EL MINISTERIO DE HACIENDA**, institución del Estado dominicano, organizado y establecido de conformidad con la Ley núm. 494-06, ubicado en la avenida México núm. 45, sector Gascue, Santo Domingo de Guzmán, Distrito Nacional, capital de la República Dominicana, debidamente representada por el señor **FRIXO MESSINA ARVELO**, Viceministro Técnico Administrativo, dominicano, mayor de edad, titular de la cédula de identidad y electoral núm. 001-0130166-1, con domicilio en esta ciudad de Santo Domingo de Guzmán, Distrito Nacional, capital de la República Dominicana, quien actúa en virtud de la Resolución núm. 195-2020 de fecha diecinueve (19) de agosto de dos mil veinte (2020), emitida por este Ministerio, quien en lo adelante se denominará como «**LA ENTIDAD CONTRATANTE**», o por su nombre completo; y

De la otra parte, la sociedad comercial **IQTEK SOLUTIONS, S. R. L.**, constituida de conformidad con la leyes de la República Dominicana, provista del Registro Nacional de Contribuyente (R. N. C.) núm. 1-30-87696-7, con su domicilio social situado en la calle Galá núm. 8, sector Arroyo Hondo Viejo, Santo Domingo de Guzmán, Distrito Nacional, capital de la República Dominicana, debidamente representada por el señor **FRANKLYN GEOVANNY CIPRIAN GOODIN**, dominicano, mayor de edad, titular de la cédula de identidad núm. 001-0908680-1, domiciliado y residente en esta ciudad de Santo Domingo de Guzmán, Distrito Nacional, capital de la República Dominicana, quien actúa en virtud del Acta de la Asamblea General Extraordinaria de fecha trece (13) de enero de dos mil veinte (2020), quien para los fines del presente contrato, se denominará "**LA PRESTADORA DE SERVICIO**", o por su nombre completo.

Para referirse a ambos se les denominará **LAS PARTES.**

PREÁMBULO

POR CUANTO: que la Ley núm. 340-06, de fecha dieciocho (18) de agosto de dos mil seis (2006), sobre Compras y Contrataciones Públicas de Bienes, Servicios, Obras y Concesiones, y su posterior modificación contenida en la Ley núm. 449-06, de fecha seis (6) de diciembre de dos mil seis (2006), establece entre los Procedimientos de Selección la Licitación Pública Nacional.

POR CUANTO: que la referida Ley, en el numeral 1 del artículo 16, establece además que: «Licitación Pública: Es el procedimiento administrativo mediante el cual las entidades del Estado realizan un llamado público abierto, convocando a los interesados para que formulen propuestas, entre los cuales seleccionará la más conveniente conforme a los pliegos de condiciones correspondiente».

POR CUANTO: que el artículo 17 de la referida Ley, establece la tabla contentiva de los factores mediante la cual se determina los umbrales topes que sirven de base para la selección del procedimiento a aplicar en un proceso de compra o contratación.

POR CUANTO: que la Resolución núm. PNP-01-2020, de fecha siete (7) de enero de dos mil veinte (2020), emitida por la Dirección General de Contrataciones Públicas, indica los umbrales para la determinación de los procedimientos de compras y contrataciones durante el ejercicio correspondiente al año dos mil veinte (2020), y establece que toda compra o contratación de

CONSORCIO EMDOC Santo Domingo, R.D.

bienes y servicios que comprenda un monto desde cuatro millones cuatrocientos un mil seiscientos veintinueve pesos dominicanos con cero centavos (RD$4,401,629.00), en adelante, deberá realizarse bajo la modalidad de Licitación Pública Nacional.

POR CUANTO: que mediante el Acto Administrativo núm. 072-2020, de fecha veintinueve (29) de diciembre de dos mil veinte (2020), el Comité de Compras y Contrataciones de este Ministerio, autorizó el Procedimiento de Licitación Pública Nacional, aprobó el Pliego de Condiciones Específicas y designó los peritos técnicos para la «Solicitud de renovación de soporte y mantenimiento soluciones informáticas del Ministerio de Hacienda, Referencia núm. MH-CCC-LPN-2020-0003».

POR CUANTO: que después de un minucioso estudio de las propuestas técnicas «Sobres A» y económicas «Sobres B» presentadas por los oferentes participantes, el Comité de Compras y Contrataciones de este Ministerio de Hacienda, mediante el Acto Administrativo núm. 006-2021, de fecha cuatro (4) de marzo de dos mil veintiuno (2021), adjudicó al oferente **IQTEK SOLUTIONS, S. R. L.**, el Lote II: Soporte y mantenimiento de HPE, del Procedimiento de Licitación Pública Nacional de Referencia núm. MH-CCC-LPN-2020-0003.

POR CUANTO: que, en ese sentido, en fecha once (11) de marzo de dos mil veintiuno (2021), **LA ENTIDAD CONTRATANTE** procedió a la notificación de los resultados finales del citado procedimiento a los oferentes participantes.

POR CUANTO: que en fecha doce (12) de marzo de dos mil veintiuno (2021), **LA PRESTADORA DE SERVICIO** constituyó la Garantía de Fiel Cumplimiento de Contrato, Póliza núm. FIAN-15542, con la entidad Seguros Sura, S. A., correspondiente al cuatro por ciento (4%) del monto total adjudicado, en cumplimiento a las disposiciones del artículo 112, del Decreto núm. 543-12, de fecha seis (6) de septiembre de dos mil doce (2012) contentivo del Reglamento de Aplicación de la Ley núm. 340-06 y sus modificaciones.

POR LO TANTO, y en el entendido de que el anterior preámbulo forma parte integral del presente Contrato.

LAS PARTES HAN CONVENIDO Y PACTADO LO SIGUIENTE:

ARTÍCULO 1.- DEFINICIONES:

Siempre que en el presente Contrato se empleen los siguientes términos, se entenderá que significan lo que expresa a continuación:

a) **Contrato**: el presente documento.
b) **Coordinador**: la persona física que actúa en nombre y representación de **LA ENTIDAD CONTRATANTE** para la coordinación de los servicios.
c) **La Prestadora de Servicio**: nombre de la persona natural o jurídica, consorcio, que ejecutará el objeto del Contrato.
d) **Entidad Contratante**: **EL MINISTERIO DE HACIENDA**.
e) **Máxima Autoridad Ejecutiva**: el titular o representante legal de **EL MINISTERIO DE HACIENDA**.
f) **Monto del Contrato**: el importe señalado en el contrato.
g) **Oferente/Proponente**: persona natural o jurídica que presenta credenciales a los fines de participar en un procedimiento de contratación.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

ARTÍCULO 2.- DOCUMENTOS CONSTITUYENTES DEL CONTRATO:

Los siguientes documentos forman parte integral e insustituible del presente Contrato, y **LA PRESTADORA DE SERVICIO** reconoce cada uno de estos como parte intrínseca del mismo:

a) El Contrato.
b) El Pliego de Condiciones Específicas del procedimiento.
c) La Oferta Técnica «Sobre A» y la Oferta Económica «Sobre B» presentadas por la **LA PRESTADORA DE SERVICIO**.
d) Documentos de **LA PRESTADORA DE SERVICIO**; y
e) Garantía de Fiel Cumplimiento del Contrato.

ARTÍCULO 3.- OBJETO DEL CONTRATO:

LA PRESTADORA DE SERVICIO, por medio del presente Contrato se compromete a cumplir con todos los requisitos establecidos en el Pliego de Condiciones Específicas correspondiente al Lote II: Soporte y mantenimiento de HPE del Procedimiento de Licitación Pública Nacional para la «Solicitud de renovación de soporte y mantenimiento soluciones informáticas del Ministerio de Hacienda, Referencia núm. MH-CCC-LPN-2020-0003». Asimismo, se compromete a cumplir con todo lo presentado en sus ofertas.

ARTÍCULO 4.- MONTO DEL CONTRATO:

El monto total convenido para la prestación de servicios objeto del presente Contrato, asciende a la suma de **DOS MILLONES SEISCIENTOS CINCUENTA Y CINCO MIL QUINIENTOS SETENTA Y TRES PESOS DOMINICANOS CON 89/100 CENTAVOS (RD$2,655,573.89)**, este monto incluye Impuesto sobre Transferencia de Bienes Industrializados y Servicios (ITBIS).

ARTICULO 5.- FORMA DE PAGO:

5.1 El pago será realizado en pesos dominicanos.

5.2 La **ENTIDAD CONTRATANTE** establece la siguiente modalidad de pago: el cien por ciento (100%) del monto total del Contrato, se pagará dentro de los treinta (30) días siguientes luego de emitida la factura, por concepto de soportes y mantenimientos, de acuerdo a la sección 2.8 sobre Descripción del Servicio contenido en el Pliego de Condiciones Específicas del Procedimiento.

ARTÍCULO 6.- TIEMPO DE VIGENCIA:

El presente contrato tendrá una vigencia de un (1) año, contado a partir del día diecinueve (19) de marzo de dos mil veintiuno (2021) hasta el día diecinueve (19) de marzo de dos mil veintidós (2022) o hasta la recepción conforme de los servicios objeto del presente Contrato.

ARTÍCULO 7.- NO RELACIÓN LABORAL:

7.1 LAS PARTES aceptan y reconocen que el presente Contrato no establece una relación de subordinación laboral entre ellas bajo el Código de Trabajo de la República Dominicana.

CONSORCIO E... EMDOC CONSORCIO Santo Domingo, R.D.

7.2 LAS PARTES acuerdan, por este medio, liberarse mutuamente de toda acción o demanda laboral que ella o su personal, sus empleados y representantes intentaren en su contra, derivada del cumplimiento y ejecución del presente Contrato.

ARTÍCULO 8.- FUERZA MAYOR Y CASO FORTUITO:

8.1 Ni **LA ENTIDAD CONTRATANTE** ni **LA PRESTADORA DE SERVICIO** serán responsables de cualquier incumplimiento de El Contrato si su ejecución ha sido demorada, impedida, obstaculizada o frustrada por causas de Fuerza Mayor o Caso Fortuito.

8.2 Para los efectos del presente Contrato, Fuerza Mayor significa cualquier evento o situación que escapen al control de una parte, imprevisible e inevitable, y sin que esté envuelta su negligencia o falta, como son, a manera enunciativa pero no limitativa, actos de autoridades gubernamentales o militares, regulaciones o requerimientos gubernamentales, epidemias, guerras, actos de terroristas, huelgas, fuegos, explosiones, temblores de tierra, accidentes, catástrofes, inundaciones y otras perturbaciones ambientales mayores, condiciones severas e inusuales del tiempo.

8.3 Caso Fortuito significa aquel acontecimiento que no ha podido preverse, o que previsto no ha podido evitarse, por ser extraño a la voluntad de las personas.

8.4 Las causas de Fuerza Mayor o Caso Fortuito especificadas anteriormente no incluyen:

1. Cualquier evento causado por negligencia o acción intencional de una parte.
2. Cualquier evento que una de las partes pudo haber tomado en cuenta al momento de la firma o de la ejecución de este Contrato para evitar incumplimiento de sus obligaciones.
3. Insuficiencia de recursos o fallas en el cumplimiento de cualquier pago bajo este Contrato.

8.5 La falla de una parte involucrada en el presente Contrato, que le impida cumplir cualquiera de sus obligaciones, no será considerada como incumplimiento, siempre y cuando éste surja de un evento de Fuerza Mayor o Caso Fortuito y la parte afectada haya tomado todas las precauciones razonables, con el debido esmero y cuidado, siempre con el objetivo de cumplir con los términos y condiciones establecidos en este Contrato.

8.6 Si por una causa de Fuerza Mayor o Caso Fortuito, **LA PRESTADORA DE SERVICIO** no concluye sus labores en el plazo establecido, **LA ENTIDAD CONTRATANTE** extenderá el Contrato por un tiempo igual al periodo en el cual **LA PRESTADORA DE SERVICIO** no pudo cumplir, debido únicamente a esta causa.

8.7 **LA PRESTADORA DE SERVICIO** tendrá derecho al pago o los pagos establecidos en el presente Contrato durante el periodo de incumplimiento como resultado de una causa de Fuerza Mayor o Caso Fortuito. Igualmente tendrá derecho al reembolso de cualquier gasto

adicional directamente relacionado con las obligaciones resultantes del Contrato en el que incurra durante el período de Fuerza Mayor o Caso Fortuito.

8.8 Si **LA PRESTADORA DE SERVICIO** dejara de presentar tal reclamación o de dar el aviso requerido dentro del período especificado, se considerará como que ha renunciado a su

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

derecho en relación a la ocurrencia de la Fuerza Mayor o Caso Fortuito.

ARTÍCULO 9.- MEDIDAS A TOMAR:

LAS PARTES acuerdan que:

a) La parte afectada por un evento de Fuerza Mayor o Caso Fortuito deberá tomar las medidas razonables para suprimir la inhabilidad de la otra Parte en cumplir con sus obligaciones.
b) La parte afectada por un evento de Fuerza Mayor o Caso Fortuito deberá notificar, en un plazo no mayor de veinticuatro (24) horas y por escrito a la otra parte la ocurrencia del evento, indicando su naturaleza y causa; de igual manera deberá notificar por escrito a la otra parte la restauración de las condiciones normales tan pronto se resuelva la situación de Fuerza Mayor o Caso Fortuito.
c) Las partes adoptarán todas las medidas posibles para reducir las consecuencias adversas de un evento de Fuerza Mayor o Caso Fortuito.

ARTÍCULO 10.- OBLIGACIONES DE LA PRESTADORA DE SERVICIO:

10.1 **LA PRESTADORA DE SERVICIO** prestará los servicios previstos en el presente Contrato como se describen en el Pliego de Condiciones Específicas.

10.2 **LA PRESTADORA DE SERVICIO** presentará a **LA ENTIDAD CONTRATANTE**, de su propia iniciativa o a solicitud de aquella, todas las informaciones y aclaraciones relacionadas con la ejecución del Contrato.

10.3 **LA PRESTADORA DE SERVICIO** realizará los servicios y cumplirá sus obligaciones establecidas bajo este Contrato con diligencia, eficiencia y economía, conforme a las normas y prácticas generalmente aceptadas y a las normas para el ejercicio del servicio contratado, reconocidas por los organismos internacionales y nacionales. Asimismo, empleará métodos ortodoxos de administración y utilizará la tecnología avanzada más adecuada, así como los equipos, maquinarias y materiales más seguros y eficaces durante el desempeño de su gestión.

10.4 **LA PRESTADORA DE SERVICIO** ejecutará y concluirá sus servicios y subsanará cualquier deficiencia en los mismos identificadas por **LA ENTIDAD CONTRATANTE** con el cuidado y la diligencia debidos y en riguroso cumplimiento de las disposiciones del Contrato.

10.5 **LA PRESTADORA DE SERVICIO** se atendrá a las órdenes administrativas impartidas por **LA ENTIDAD CONTRATANTE**. Cuando **LA PRESTADORA DE SERVICIO** considere que las exigencias de una orden administrativa sobrepasan El Contrato, deberá notificarlo a **LA ENTIDAD CONTRATANTE** en un plazo de quince (15) días a partir del recibo de la orden administrativa. La ejecución de la orden administrativa no se suspenderá como consecuencia de dicha notificación.

10.6 **LA PRESTADORA DE SERVICIO** respetará y cumplirá toda la legislación y normativa vigente en el Estado dominicano.

ARTÍCULO 11.- CONFLICTO DE INTERESES:

LA PRESTADORA DE SERVICIO no se beneficiará de otros pagos. El pago a ser recibido por

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

LA PRESTADORA DE SERVICIO previsto en el artículo 4 del presente Contrato, constituye la única remuneración con relación al alcance del mismo. Por tanto, **LA PRESTADORA DE SERVICIO** no podrá exigir ningún pago adicional por ningún concepto en relación con las actividades establecidas en este Contrato o en cumplimiento de sus obligaciones. Además, **LA PRESTADORA DE SERVICIO** utilizará sus mejores esfuerzos para asegurar que su personal técnico tampoco reciba remuneración adicional a la prevista en este Contrato.

ARTÍCULO 12 - PROHIBICIÓN DE ACTIVIDADES CONFLICTIVAS:

Ni **LA PRESTADORA DE SERVICIO** ni su personal técnico acreditado tendrán derecho a comprometerse, directa o indirectamente, en cualquier negocio o actividad profesional que pueda producir un conflicto de intereses con las responsabilidades puestas a su cargo en virtud de este Contrato.

ARTÍCULO 13.- CONFIDENCIALIDAD:

Todos los informes y documentos que se produzcan como consecuencia del presente Contrato no podrán ser divulgados a terceras personas o instituciones, durante ni después de la expiración del presente Contrato, sin la autorización escrita de **LAS PARTES**.

ARTÍCULO 14 - GARANTÍA DE FIEL CUMPLIMIENTO DE CONTRATO:

Para garantizar el fiel cumplimiento del presente contrato, **LA PRESTADORA DE SERVICIO**, en fecha doce (12) de marzo de dos mil veintiuno (2021), hace formal entrega de la Póliza núm. FIAN-15542, expedida por Seguros Sura, S. A., a favor de **LA ENTIDAD CONTRATANTE**, en cumplimiento con lo establecido en el artículo 112 del Reglamento de Aplicación de la Ley núm. 340 y sus modificaciones, aprobado mediante Decreto núm. 543-12.

PÁRRAFO I. La garantía del fiel cumplimiento de contrato responderá por los daños y perjuicios que experimente **EL MINISTERIO DE HACIENDA** en caso de incumplimiento por parte de **IQTEK SOLUTIONS, S. R. L.,** de las disposiciones contenidas en este contrato, toda vez que el mismo no sea por una causa justificada, notificada oportunamente a **LA ENTIDAD CONTRATANTE** o por causa de fuerza mayor. De comprobarse el incumplimiento, **EL MINISTERIO DE HACIENDA** procederá a ejecutar la garantía, independientemente de las acciones judiciales que correspondan.

PÁRRAFO II. La garantía solicitada ha sido expedida por una compañía de seguro del mercado dominicano, Seguros Sura, S. A., de acuerdo a la última publicación realizada por la Superintendencia de Seguros.

PÁRRAFO III. En caso de que a la llegada del término de la vigencia de esta garantía se continúe prestando los servicios objeto de este contrato **IQTEK SOLUTIONS, S. R. L.**, queda obligada a renovarla automáticamente por el período que fuera acordado entre **LAS PARTES.**

PÁRRAFO IV. Dicha garantía responderá de los daños y perjuicios que se produzcan a **LA ENTIDAD CONTRATANTE** en caso de incumplimiento, que determinará en todo caso la ejecución de la Garantía, independientemente del resto de acciones que legalmente procedan.

ARTÍCULO 15.- INDEMNIZACIÓN POR PARTE DE LA PRESTADORA DE SERVICIO:

LA PRESTADORA DE SERVICIO será responsable dentro de los límites de su seguro de

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

responsabilidad civil general, de indemnizar a **LA ENTIDAD CONTRATANTE** total y efectivamente contra toda pérdida, daños, perjuicios, muertes, gastos, acción, procedimiento, demanda, costos y reclamaciones de una tercera persona, ocurrida durante la vigencia del presente Contrato, incluyendo, pero sin limitar, a honorarios y gastos legales incurridos por **LA ENTIDAD CONTRATANTE,** pero solamente en la medida en que tales pérdidas, daños, o perjuicios sean resultado de actos ilícitos o negligencia de **LA PRESTADORA DE SERVICIO,** así como del uso o violación de cualquier patente de invención o propiedad intelectual o de cualquier hecho o acontecimiento que resulte como consecuencia de su falta

ARTÍCULO 16.- OBLIGACIONES DE LA ENTIDAD CONTRATANTE:

LA ENTIDAD CONTRATANTE hará sus mejores esfuerzos para asegurar que:

a) Provea a **LA PRESTADORA DE SERVICIO** y a su personal técnico acreditado de cualquier documento gubernamental necesario para la realización de los servicios establecidos en este Contrato;

b) Emita las instrucciones necesarias a los agentes, funcionarios y representantes del Estado para la rápida y efectiva ejecución de los servicios;

ARTÍCULO 17.- EQUILIBRIO ECONÓMICO:

Si en fecha posterior a la entrada en vigencia del presente Contrato se producen cambios en las leyes nacionales, relativos y relacionados con la moneda nacional, que impliquen aumentos en el costo o en los gastos a incurrir por **LA PRESTADORA DE SERVICIO** para la realización de sus servicios, los pagos y los gastos reembolsables pagables a **LA PRESTADORA DE SERVICIO** en virtud de este Contrato aumentarán en la proporción correspondiente a las modificaciones que haya sufrido la legislación con relación a la devaluación de la moneda nacional.

ARTÍCULO 18.- MODIFICACIONES AL CONTRATO:

Cualquier modificación a los términos y condiciones del presente Contrato deberá hacerse por acuerdo mutuo entre **LAS PARTES**, por escrito, mediante enmiendas numeradas cronológicamente y la fecha de vigencia de cada una se contará a partir de la fecha de aprobación realizada por **LA ENTIDAD CONTRATANTE.**

ARTÍCULO 19.- SUSPENSIÓN:

Por parte de **LA ENTIDAD CONTRATANTE:**

LA ENTIDAD CONTRATANTE tendrá derecho a suspender los pagos e inclusive sus servicios a **LA PRESTADORA DE SERVICIO** mediante notificación escrita si **LA PRESTADORA DE SERVICIO** incumple sus obligaciones establecidas bajo este Contrato, siempre y cuando la notificación de la suspensión:

(i) Especifique la naturaleza del incumplimiento, y
(ii) Requiera que **LA PRESTADORA DE SERVICIO** resuelva el incumplimiento dentro de un periodo no mayor de diez (10) días hábiles a partir del recibo de la notificación de suspensión.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

Por parte de **LA PRESTADORA DE SERVICIO**:

LA PRESTADORA DE SERVICIO tendrá derecho a suspender la prestación de sus servicios mediante notificación por escrito a **LA ENTIDAD CONTRATANTE**, si ésta incumple sus obligaciones establecidas en virtud de este Contrato, siempre y cuando la notificación de la suspensión:

(i) Especifique la naturaleza del incumplimiento; y
(ii) Requiera que **LA ENTIDAD CONTRATANTE** resuelva el incumplimiento dentro de un período no mayor de diez (10) días hábiles a partir del recibo por parte de **LA ENTIDAD CONTRATANTE** de la notificación de suspensión.

La suspensión se aplicará a partir de la fecha de vencimiento del plazo indicado en la notificación.

ARTÍCULO 20.- RESCISIÓN DEL CONTRATO:

LA ENTIDAD CONTRATATANTE podrá rescindir el presente Contrato unilateralmente en el caso de falta grave de **LA PRESTADORA DE SERVICIO** y siempre que la misma no sea originada por acontecimientos de Fuerza Mayor o Caso Fortuito. En este caso, **LA ENTIDAD CONTRATATANTE** no compensará por ningún motivo a **LA PRESTADORA DE SERVICIO** por las sumas adeudadas.

LA ENTIDAD CONTRATATANTE podrá rescindir, sin responsabilidad ninguna, el presente Contrato, así como ejecutar la Fianza de Fiel Cumplimiento de Contrato, si **LA PRESTADORA DE SERVICIO** fuese a la quiebra, o si se extendiese contra él una orden de administración judicial, o si se presentase una petición de declaración en quiebra, o si hiciese algún convenio con sus acreedores o una cesión a favor de ellos.

En el caso en que **LA PRESTADORA DE SERVICIO** desee renunciar o que ambas partes deseen rescindir el Contrato por acuerdo mutuo, **LA ENTIDAD CONTRATATANTE** compensará a **LA PRESTADORA DE SERVICIO** de acuerdo al tiempo y al servicio suministrado objeto del presente contrato que haya sido ejecutado a la fecha.

ARTÍCULO 21.- CESE DE DERECHOS:

Con la rescisión del presente Contrato, conforme lo establecido en el artículo que antecede, cesan todos los derechos y obligaciones a excepción de:

(i) Aquellos derechos y obligaciones de **LAS PARTES** que estén pendientes a la fecha de rescisión o terminación; y

(ii) La obligación de confidencialidad a que se refiere el artículo 13.

ARTÍCULO 22.- CESIÓN DE CONTRATO:

La capacidad técnica de **LA PRESTADORA DE SERVICIO** es el objetivo esencial de la utilización de sus servicios, por tanto, éste Contrato no podrá ser cedido, ni en todo ni en parte, sin la autorización previa por escrito de **LA ENTIDAD CONTRATATANTE**. No obstante, **LA PRESTADORA DE SERVICIO** podrá utilizar los servicios de otra firma asociada para el cumplimiento del mismo sin costo adicional para **LA ENTIDAD CONTRATATANTE.**

ARTÍCULO 23.- NULIDADES DEL CONTRATO:

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

890

La violación del régimen de prohibiciones establecido en el artículo 14 de la Ley núm. 340-06 y sus modificaciones, originará la nulidad absoluta del Contrato, sin perjuicio de otra acción que decida interponer **LA ENTIDAD CONTRATATANTE.**

La división del presente Contrato, con el fin de evadir las obligaciones de la Ley 340-06 núm. 340- 06 y sus modificaciones, y de las normas complementarias que se dicten en el marco del mismo, será causa de nulidad del mismo

ARTÍCULO 24.- ARREGLO DE CONFLICTOS:

LAS PARTES se comprometen a realizar sus mejores esfuerzos para resolver en forma amigable los conflictos o desacuerdos que pudieran surgir con relación al desarrollo del presente Contrato y su interpretación.

ARTÍCULO 25.- SOLUCIÓN DE CONTROVERSIAS:

Todo litigio, controversia o reclamación resultante de este Contrato o relativo al mismo, su incumplimiento, su interpretación, su resolución o nulidad será sometido al Tribunal Contencioso, Tributario, Administrativo, instituido mediante la Ley núm. 13-07, de fecha cinco (05) de febrero de dos mil siete (2007).

ARTÍCULO 26.- INTERPRETACIÓN DEL CONTRATO.

El significado e interpretación de los términos y condiciones del presente Contrato se hará al amparo de las leyes de la República Dominicana.

ARTÍCULO 27.- IDIOMA OFICIAL:

El presente Contrato ha sido redactado en español, que será el idioma de control para todos los asuntos relacionados con el significado e interpretación de los términos y condiciones del presente documento.

ARTÍCULO 28.- TITULOS:
Los títulos no limitarán, alterarán o modificarán el significado de este Contrato.

ARTÍCULO 29.- LEGISLACIÓN APLICABLE:

LA PRESTADORA DE SERVICIO realizará sus servicios de conformidad con las leyes nacionales y tomará todas las medidas necesarias para asegurar que su personal técnico cumpla con las leyes vigentes en la República Dominicana.

ARTÍCULO 30.- ELECCIÓN DE DOMICILIO:

Para todos los fines y consecuencias del presente Contrato, **LAS PARTES** eligen domicilio en las direcciones que figuran en la parte introductora del presente Contrato, en el cual recibirán válidamente todo tipo de correspondencia o notificación relativa al presente Contrato, su ejecución y terminación.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

891

ARTÍCULO 31.- ACUERDO ÍNTEGRO:

El presente Contrato y sus anexos contienen todas las estipulaciones y acuerdos convenidos entre **LAS PARTES**; en caso de ambigüedad, duda o desacuerdo sobre la interpretación del mismo y sus documentos anexos, prevalecerá su redacción. Asimismo, se establece que, si alguna de las disposiciones de este Contrato se declarara inválida, las demás no serán afectadas y permanecerán plenamente vigentes.

HECHO Y FIRMADO en la ciudad de Santo Domingo de Guzmán, Distrito Nacional, capital de la República Dominicana, a los diecinueve (19) días del mes de marzo del año dos mil veintiuno (2021), en tres (3) originales del mismo tenor y efecto, uno para cada una de las partes y el otro para los fines legales correspondientes.

FRIXO MESSINA ARVELO
Actuando a nombre y representación de
EL MINISTERIO DE HACIENDA

FRANKLYN GEOVANNY CIPRIAN GOODIN
Actuando en nombre y representación de
IQTEK SOLUTIONS, S. R. L.

IQtek Solutions, S.R.L. RNC: 130816987 Santo Domingo, R.D.

DR. JOSE MIGUEL DE HERRERA BUENO ABOGADO NOTARIO PUBLICO COLEGIATURA 4622 SANTO DOMINGO, R.D.

José M. de Herrera B., Abogado Notario Público de los del número del Distrito Nacional, provisto de la matrícula núm. 4622 **CERTIFICO Y DOY FE**, que las firmas de los señores **FRIXO MESSINA ARVELO** y **FRANKLYN GEOVANNY CIPRIAN GOODIN**, fueron puestas en mi presencia libre y voluntariamente, quienes me declararon que esas firmas son las que usan en los documentos de sus vidas públicas y privadas, por lo que merecen entera fe y crédito. En la ciudad de Santo Domingo de Guzmán, Distrito Nacional, capital de la República Dominicana, a los diecinueve (19) días del mes de marzo del año dos mil veintiuno (2021).

NOTARIO PUBLICO

DR. JOSE MIGUEL DE HERRERA BUENO ABOGADO NOTARIO PUBLICO COLEGIATURA 4622 SANTO DOMINGO, R.D.

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

892

EMDOC
CONSORCIO

Cartas o
Declaraciones Juradas

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

EMDOC
CONSORCIO

DECLARACIÓN JURADA

Quien suscribe, **BERNARDO ANTONIO PÉREZ DIAZ**, dominicano, mayor de edad, casado, portador de la Cédula de Identidad y Electoral No. 001-0196576-2, domiciliado y residente en esta ciudad de Santo Domingo de Guzmán, Distrito Nacional, capital de la República Dominicana, actuando en calidad de representante del **CONSORCIO EMDOC**, conformado por:

1. **IQTEK SOLUTIONS, S.R.L.**, Sociedad de Responsabilidad Limitada, constituida de conformidad con las leyes de la República Dominicana, Registro Mercantil No. 87130SD, Registro Nacional de Contribuyentes (RNC) No. 1-30-87696-7, con domicilio social en la Calle Galá No. 8, sector Arroyo Hondo Viejo, Santo Domingo de Guzmán, Distrito Nacional;

2. **ULTRA TECH INC, S.A.**, persona jurídica constituida de conformidad con las leyes de la República de Panamá, inscrita en el Registro Público de Panamá, Folio 754130 (S) de la sección mercantil del registro público, al viernes 2 de diciembre de 2011, con domicilio social en , Calle 50 con Calle 56, Edificio F&F Tower, piso 47, oficina 47 C y D, Ciudad de Panamá, República de Panamá;

3. **GSI INTERNATIONAL, INC.**, sociedad de comercio de nacionalidad Panameña, organizada y existente de conformidad con las leyes de la República Dominicana, provista del Registro Nacional de Contribuyentes (RNC) No. 1-3014306-4, e inscrita en el Registro Mercantil con el No. 32067SD, y domicilio social en la Avenida 27 de febrero, esquina Tiradentes, Torre Empresarial Friusa, piso 8, suite 8B, La Esperilla;

4. **MÜHLBAUER ID SERVICES GMBH.**, sociedad de responsabilidad limitada constituida con arreglo a las leyes de la República Federal de Alemania, registrada en el Tribunal de Distrito de Ratisbona (Alemania) con el número HRB 9094, número de identificación a efectos del IVA VAT DE 813871380, con domicilio social en Josef-Mühlbauer-Platz 1, 93426 Roding, Alemania,

5. **VERIDOS GMBH**, sociedad de responsabilidad limitada, constituida según las leyes de Alemania, registrada en Juzgado Local de Charlottenburg, bajo el número HRB 155795 B, de Identificación Fiscal número 143/306/40066, con asiento social en Oranienstr. 91, 10969, Berlín, Alemania;

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

DECLARO BAJO LA FE DEL JURAMENTO LO SIGUIENTE:

PRIMERO: Que en nombre y representación del **CONSORCIO EMDOC** y sus miembros, reconozco y acepto que ningún oferente (de tarjetas, de impresoras, de cédula digital, de ABIS) podrá presentar más de una Oferta para el Proyecto.

SEGUNDO: Que ninguno de los miembros del **CONSORCIO EMDOC** tendrá derecho ni a presentar ni a licitar individualmente o como miembro de algún otro consorcio.

TERCERO: Que esta restricción no se aplica a los proveedores de materiales o equipos tales como equipos de infraestructura, dispositivos o consumibles.

La presente declaración se realiza para los fines requeridos para el Proceso de Licitación Pública Internacional No. **JCE-CCC-LPI-2024-0001**, en la ciudad de Santo Domingo de Guzmán, Distrito Nacional, capital de la República Dominicana, a los veinte (20) días del mes de febrero del año dos mil veinticinco (2025).

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

BERNARDO ANTONIO PÉREZ DIAZ
Representante del **CONSORCIO EMDOC**

Yo, **DRA. YILDA VERENISIA DE LEÓN**, Abogada - Notario Público de los del número del Distrito Nacional, autorizada mediante Matrícula No. 3004, **CERTIFICO Y DOY FE:** que por ante mí compareció el señor **BERNARDO ANTONIO PÉREZ DÍAZ**, de calidad que consta en el presente documento y a quien doy fe de conocer, quien me ha declarado que la firma puesta en el presente acto es la que acostumbra a utilizar en todos los actos de su vida. En la ciudad de Santo Domingo de Guzmán, Distrito Nacional, capital de la República Dominicana, a los veinte (20) días del mes de febrero del año dos mil veinticinco (2025).

YILDA VERENISIA DE LEÓN
Abogada – Notario Público

YILDA VERENISIA DE LEÓN
NOTARIO PÚBLICO DEL DISTRITO NACIONAL
3004
Santo Domingo, R.D.

EMDOC
CONSORCIO

DECLARACIÓN JURADA

Quien suscribe, **BERNARDO ANTONIO PÉREZ DIAZ**, dominicano, mayor de edad, casado, portador de la Cédula de Identidad y Electoral No. 001-0196576-2, domiciliado y residente en esta ciudad de Santo Domingo de Guzmán, Distrito Nacional, capital de la República Dominicana, actuando en calidad de representante del **CONSORCIO EMDOC**, conformado por:

1. **IQTEK SOLUTIONS, S.R.L.**, Sociedad de Responsabilidad Limitada, constituida de conformidad con las leyes de la República Dominicana, Registro Mercantil No. 87130SD, Registro Nacional de Contribuyentes (RNC) No. 1-30-87696-7, con domicilio social en la Calle Galá No. 8, sector Arroyo Hondo Viejo, Santo Domingo de Guzmán, Distrito Nacional;

2. **ULTRA TECH INC, S.A.**, persona jurídica constituida de conformidad con las leyes de la República de Panamá, inscrita en el Registro Público de Panamá, Folio 754130 (S) de la sección mercantil del registro público, al viernes 2 de diciembre de 2011, con domicilio social en , Calle 50 con Calle 56, Edificio F&F Tower, piso 47, oficina 47 C y D, Ciudad de Panamá, República de Panamá;

3. **GSI INTERNATIONAL, INC.**, sociedad de comercio de nacionalidad Panameña, organizada y existente de conformidad con las leyes de la República Dominicana, provista del Registro Nacional de Contribuyentes (RNC) No. 1-3014306-4, e inscrita en el Registro Mercantil con el No. 32067SD, y domicilio social en la Avenida 27 de febrero, esquina Tiradentes, Torre Empresarial Friusa, piso 8, suite 8B, La Esperilla;

4. **MÜHLBAUER ID SERVICES GMBH.**, sociedad de responsabilidad limitada constituida con arreglo a las leyes de la República Federal de Alemania, registrada en el Tribunal de Distrito de Ratisbona (Alemania) con el número HRB 9094, número de identificación a efectos del IVA VAT DE 813871380, con domicilio social en Josef-Mühlbauer-Platz 1, 93426 Roding, Alemania,

5. **VERIDOS GMBH,** sociedad de responsabilidad limitada, constituida según las leyes de Alemania, registrada en Juzgado Local de Charlottenburg, bajo el número HRB 155795 B, de Identificación Fiscal número 143/306/40066, con asiento social en Oranienstr. 91, 10969, Berlín, Alemania;

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, RD

Por este medio de la presente **DECLARO BAJO LA FE DEL JURAMENTO** que se analizaron los Estados Financieros de los años 2021,2022 y 2023 de las empresas que conforman el CONSORCIO EMDOC, por ende, declaramos que cumplimos con los requisitos de solvencia, por lo que que acreditamos ser mayor que una. (Ver adjuntos)

La presente declaración se realiza para los fines requeridos para el Proceso de Licitación Pública Internacional No. **JCE-CCC-LPI-2024-0001**, en la ciudad de Santo Domingo de Guzmán, Distrito Nacional, capital de la República Dominicana, a los veinte (20) días del mes de febrero del año dos mil veinticinco (2025).

CONSORCIO EMDOC
EMDOC
Santo Domingo, R.D.

BERNARDO ANTONIO PÉREZ DIAZ
Representante del **CONSORCIO EMDOC**

Yo, **DRA. YILDA VERENISIA DE LEÓN**, Abogada - Notario Público de los del número del Distrito Nacional, autorizada mediante Matrícula No. 3004, **CERTIFICO Y DOY FE:** que por ante mí compareció el señor **BERNARDO ANTONIO PÉREZ DÍAZ**, de calidad que consta en el presente documento y a quien doy fe de conocer, quien me ha declarado que la firma puesta en el presente acto es la que acostumbra a utilizar en todos los actos de su vida. En la ciudad de Santo Domingo de Guzmán, Distrito Nacional, capital de la República Dominicana, a los veinte (20) días del mes de febrero del año dos mil veinticinco (2025).

YILDA VERENISIA DE LEÓN
Abogada – Notario Público

EMDOC
CONSORCIO

25 de febrero de 2025

Señores
Junta Central Electoral
Santo Domingo, R. D.

Atención: **Comité de Compras y Contrataciones**

Referencia: **JCE-CCC-LPI-2024-0001**

Distinguidos señores:

Quien suscribe, Señor **Bernardo Antonio Pérez Diaz**, dominicano, mayor de edad, estado civil casado, portador de la Cédula de Identidad y Electoral No. 001-0196576-2, domiciliado y residente en Santo Domingo, actuando en nombre y representación del **CONSORCIO EMDOC**, tengo a bien presentar un consolidado de partidas de los Estados Financieros de los Consorciados, detallado en la siguiente tabla:

CONSOLIDADO PARTIDAS DE LOS ESTADOS FINANCIEROS DE LOS CONSORCIADOS
Razones e Indices Financieros

DETALLE	2023	COEFICIENTE	2022	COEFICIENTE	2021	COEFICIENTE	FORMULA	INDICES
Activo total	149,507,152,562	1.59	99,727,612,523	1.66	172,878,912,294	1.39	ACTIVO TOTAL/PASIVO TOTAL	Solvencia > 1
Deuda total	93,961,393,278		59,947,658,268		124,042,242,705			

Sirviendo esta comunicación como parte integral de la Declaración Jurada firmada en fecha veinte (20) del mes de febrero del año dos mil veinticinco (2025).

Se despide,

Bernardo Pérez
Apoderado Legal
Consorcio EMDOC

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

EMDOC
CONSORCIO

DECLARACIÓN JURADA

Quien suscribe, **BERNARDO ANTONIO PÉREZ DIAZ**, dominicano, mayor de edad, casado, portador de la Cédula de Identidad y Electoral No. 001-0196576-2, domiciliado y residente en esta ciudad de Santo Domingo de Guzmán, Distrito Nacional, capital de la República Dominicana, actuando en calidad de representante del **CONSORCIO EMDOC**, conformado por:

1. **IQTEK SOLUTIONS, S.R.L.**, Sociedad de Responsabilidad Limitada, constituida de conformidad con las leyes de la República Dominicana, Registro Mercantil No. 87130SD, Registro Nacional de Contribuyentes (RNC) No. 1-30-87696-7, con domicilio social en la Calle Galá No. 8, sector Arroyo Hondo Viejo, Santo Domingo de Guzmán, Distrito Nacional;

2. **ULTRA TECH INC, S.A.**, persona jurídica constituida de conformidad con las leyes de la República de Panamá, inscrita en el Registro Público de Panamá, Folio 754130 (S) de la sección mercantil del registro público, al viernes 2 de diciembre de 2011, con domicilio social en , Calle 50 con Calle 56, Edificio F&F Tower, piso 47, oficina 47 C y D, Ciudad de Panamá, República de Panamá;

3. **GSI INTERNATIONAL, INC.**, sociedad de comercio de nacionalidad Panameña, organizada y existente de conformidad con las leyes de la República Dominicana, provista del Registro Nacional de Contribuyentes (RNC) No. 1-3014306-4, e inscrita en el Registro Mercantil con el No. 32067SD, y domicilio social en la Avenida 27 de febrero, esquina Tiradentes, Torre Empresarial Friusa, piso 8, suite 8B, La Esperilla;

4. **MÜHLBAUER ID SERVICES GMBH.**, sociedad de responsabilidad limitada constituida con arreglo a las leyes de la República Federal de Alemania, registrada en el Tribunal de Distrito de Ratisbona (Alemania) con el número HRB 9094, número de identificación a efectos del IVA VAT DE 813871380, con domicilio social en Josef-Mühlbauer-Platz 1, 93426 Roding, Alemania,

5. **VERIDOS GMBH**, sociedad de responsabilidad limitada, constituida según las leyes de Alemania, registrada en Juzgado Local de Charlottenburg, bajo el número HRB 155795 B, de Identificación Fiscal número 143/306/40066, con asiento social en Oranienstr. 91, 10969, Berlín, Alemania;

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

Por este medio de la presente **DECLARO BAJO LA FE DEL JURAMENTO** que se analizaron los Estados Financieros de los años 2021,2022 y 2023 de las empresas que conforman el CONSORCIO EMDOC, y determinan que cuentan con una factura de media en los últimos 3 años en su conjunto al menos 2 veces más que la totalidad del presupuesto de su propuesta con valor en ventas ascendente a los USD 518,140,931 como Consorcio. Igualmente, declaramos que el Oferente local factura de media en los 3 últimos años más de USD$5,000,000.00, según puede apreciarse en los estados financieros auditados, la cual puede ser comprobada en el Sobre B.

La presente declaración se realiza para los fines requeridos para el Proceso de Licitación Pública Internacional No. **JCE-CCC-LPI-2024-0001**, en la ciudad de Santo Domingo de Guzmán, Distrito Nacional, capital de la República Dominicana, a los veinte (20) días del mes de febrero del año dos mil veinticinco (2025).

BERNARDO ANTONIO PÉREZ DIAZ
Representante del **CONSORCIO EMDOC**

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

Yo, **DRA. YILDA VERENISIA DE LEÓN**, Abogada - Notario Público de los del número del Distrito Nacional, autorizada mediante Matrícula No. 3004, **CERTIFICO Y DOY FE:** que por ante mí compareció el señor **BERNARDO ANTONIO PÉREZ DÍAZ**, de calidad que consta en el presente documento y a quien doy fe de conocer, quien me ha declarado que la firma puesta en el presente acto es la que acostumbra a utilizar en todos los actos de su vida. En la ciudad de Santo Domingo de Guzmán, Distrito Nacional, capital de la República Dominicana, a los veinte (20) días del mes de febrero del año dos mil veinticinco (2025).

YILDA VERENISIA DE LEÓN
Abogada – Notario Público

YILDA VERENISIA DE LEÓN
REPÚBLICA DOMINICANA
Santo Domingo, R.D.

EMDOC
CONSORCIO

DECLARACIÓN JURADA

Quien suscribe, **BERNARDO ANTONIO PÉREZ DIAZ,** dominicano, mayor de edad, casado, portador de la Cédula de Identidad y Electoral No. 001-0196576-2, domiciliado y residente en esta ciudad de Santo Domingo de Guzmán, Distrito Nacional, capital de la República Dominicana, actuando en calidad de representante del **CONSORCIO EMDOC,** conformado por:

1. **IQTEK SOLUTIONS, S.R.L.,** Sociedad de Responsabilidad Limitada, constituida de conformidad con las leyes de la República Dominicana, Registro Mercantil No. 87130SD, Registro Nacional de Contribuyentes (RNC) No. 1-30-87696-7, con domicilio social en la Calle Galá No. 8, sector Arroyo Hondo Viejo, Santo Domingo de Guzmán, Distrito Nacional;

2. **ULTRA TECH INC, S.A.,** persona jurídica constituida de conformidad con las leyes de la República de Panamá, inscrita en el Registro Público de Panamá, Folio 754130 (S) de la sección mercantil del registro público, al viernes 2 de diciembre de 2011, con domicilio social en , Calle 50 con Calle 56, Edificio F&F Tower, piso 47, oficina 47 C y D, Ciudad de Panamá, República de Panamá;

3. **GSI INTERNATIONAL, INC.,** sociedad de comercio de nacionalidad Panameña, organizada y existente de conformidad con las leyes de la República Dominicana, provista del Registro Nacional de Contribuyentes (RNC) No. 1-3014306-4, e inscrita en el Registro Mercantil con el No. 32067SD, y domicilio social en la Avenida 27 de febrero, esquina Tiradentes, Torre Empresarial Friusa, piso 8, suite 8B, La Esperilla;

4. **MÜHLBAUER ID SERVICES GMBH.,** sociedad de responsabilidad limitada constituida con arreglo a las leyes de la República Federal de Alemania, registrada en el Tribunal de Distrito de Ratisbona (Alemania) con el número HRB 9094, número de identificación a efectos del IVA VAT DE 813871380, con domicilio social en Josef-Mühlbauer-Platz 1, 93426 Roding, Alemania,

5. **VERIDOS GMBH,** sociedad de responsabilidad limitada, constituida según las leyes de Alemania, registrada en Juzgado Local de Charlottenburg, bajo el número HRB 155795 B, de Identificación Fiscal número 143/306/40066, con asiento social en Oranienstr. 91, 10969, Berlín, Alemania;

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

DECLARO BAJO LA FE DEL JURAMENTO LO SIGUIENTE:

PRIMERO: Que para acreditar la elegibilidad del **CONSORCIO EMDOC** en lo referente a la experiencia requerida en Mobile ID (Cédula Digital), informamos que **MÜHLBAUER ID SERVICES GMBH** cuenta con experiencia comprobada en la implementación y desarrollo de soluciones de Mobile ID.

SEGUNDO: Que dicha experiencia puede ser verificada mediante la documentación incluida en los requisitos de experiencia no obligatorios.

La presente declaración se realiza para los fines requeridos para el Proceso de Licitación Pública Internacional No. **JCE-CCC-LPI-2024-0001**, en la ciudad de Santo Domingo de Guzmán, Distrito Nacional, capital de la República Dominicana, a los veinte (20) días del mes de febrero del año dos mil veinticinco (2025).

CONSORCIO EMDOC
EMDOC CONSORCIO
Santo Domingo, R.D.

BERNARDO ANTONIO PÉREZ DIAZ
Representante del **CONSORCIO EMDOC**

Yo, **DRA. YILDA VERENISIA DE LEÓN**, Abogada - Notario Público de los del número del Distrito Nacional, autorizada mediante Matrícula No. 3004, **CERTIFICO Y DOY FE:** que por ante mí compareció el señor **BERNARDO ANTONIO PÉREZ DÍAZ**, de calidad que consta en el presente documento y a quien doy fe de conocer, quien me ha declarado que la firma puesta en el presente acto es la que acostumbra a utilizar en todos los actos de su vida. En la ciudad de Santo Domingo de Guzmán, Distrito Nacional, capital de la República Dominicana, a los veinte (20) días del mes de febrero del año dos mil veinticinco (2025).

DRA. YILDA VERENISIA DE LEÓN
NOTARIO PÚBLICA DEL DISTRITO NACIONAL
Santo Domingo, R.D.

YILDA VERENISIA DE LEÓN
Abogada – Notario Público

EMDOC
CONSORCIO

DECLARACIÓN JURADA

Quien suscribe, **BERNARDO ANTONIO PÉREZ DIAZ**, dominicano, mayor de edad, casado, portador de la Cédula de Identidad y Electoral No. 001-0196576-2, domiciliado y residente en esta ciudad de Santo Domingo de Guzmán, Distrito Nacional, capital de la República Dominicana, actuando en calidad de representante del **CONSORCIO EMDOC**, conformado por:

1. **IQTEK SOLUTIONS, S.R.L.**, Sociedad de Responsabilidad Limitada, constituida de conformidad con las leyes de la República Dominicana, Registro Mercantil No. 87130SD, Registro Nacional de Contribuyentes (RNC) No. 1-30-87696-7, con domicilio social en la Calle Galá No. 8, sector Arroyo Hondo Viejo, Santo Domingo de Guzmán, Distrito Nacional;

2. **ULTRA TECH INC, S.A.**, persona jurídica constituida de conformidad con las leyes de la República de Panamá, inscrita en el Registro Público de Panamá, Folio 754130 (S) de la sección mercantil del registro público, al viernes 2 de diciembre de 2011, con domicilio social en , Calle 50 con Calle 56, Edificio F&F Tower, piso 47, oficina 47 C y D, Ciudad de Panamá, República de Panamá;

3. **GSI INTERNATIONAL, INC.**, sociedad de comercio de nacionalidad Panameña, organizada y existente de conformidad con las leyes de la República Dominicana, provista del Registro Nacional de Contribuyentes (RNC) No. 1-3014306-4, e inscrita en el Registro Mercantil con el No. 32067SD, y domicilio social en la Avenida 27 de febrero, esquina Tiradentes, Torre Empresarial Friusa, piso 8, suite 8B, La Esperilla;

4. **MÜHLBAUER ID SERVICES GMBH.**, sociedad de responsabilidad limitada constituida con arreglo a las leyes de la República Federal de Alemania, registrada en el Tribunal de Distrito de Ratisbona (Alemania) con el número HRB 9094, número de identificación a efectos del IVA VAT DE 813871380, con domicilio social en Josef-Mühlbauer-Platz 1, 93426 Roding, Alemania,

5. **VERIDOS GMBH**, sociedad de responsabilidad limitada, constituida según las leyes de Alemania, registrada en Juzgado Local de Charlottenburg, bajo el número HRB 155795 B, de Identificación Fiscal número 143/306/40066, con asiento social en Oranienstr. 91, 10969, Berlín, Alemania;

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

Por este medio de la presente **DECLARO BAJO LA FE DEL JURAMENTO** lo siguiente:

PRIMERO: Que la solución propuesta por PKI, cumple con el estándar de la Certificación ISO 15408, y es compatible con ICAO para establecer un SOD activado en los datos del chip;

SEGUNDO: Que la solución propuesta ha sido sometida a pruebas internas de calidad y seguridad, garantizando su fiabilidad y capacidad operativa en condiciones de uso exigentes, con un enfoque en la protección de la privacidad de los datos y la integridad del sistema.

La presente declaración se realiza para los fines requeridos para el Proceso de Licitación Pública Internacional No. **JCE-CCC-LPI-2024-0001**, en la ciudad de Santo Domingo de Guzmán, Distrito Nacional, capital de la República Dominicana, a los veinte (20) días del mes de febrero del año dos mil veinticinco (2025).

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

BERNARDO ANTONIO PÉREZ DIAZ
Representante del **CONSORCIO EMDOC**

Yo, **DRA. YILDA VERENISIA DE LEÓN,** Abogada - Notario Público de los del número del Distrito Nacional, autorizada mediante Matrícula No. 3004, **CERTIFICO Y DOY FE:** que por ante mí compareció el señor **BERNARDO ANTONIO PÉREZ DÍAZ**, de calidad que consta en el presente documento y a quien doy fe de conocer, quien me ha declarado que la firma puesta en el presente acto es la que acostumbra a utilizar en todos los actos de su vida. En la ciudad de Santo Domingo de Guzmán, Distrito Nacional, capital de la República Dominicana, a los veinte (20) días del mes de febrero del año dos mil veinticinco (2025).

DRA. YILDA VERENISIA DE LEÓN
NOTARIO PÚBLICO DEL DISTRITO NACIONAL
Santo Domingo, R.D.

YILDA VERENISIA DE LEÓN
Abogada – Notario Público

EMDOC
CONSORCIO

DECLARACIÓN JURADA

Quien suscribe, **BERNARDO ANTONIO PÉREZ DIAZ**, dominicano, mayor de edad, casado, portador de la Cédula de Identidad y Electoral No. 001-0196576-2, domiciliado y residente en esta ciudad de Santo Domingo de Guzmán, Distrito Nacional, capital de la República Dominicana, actuando en calidad de representante del **CONSORCIO EMDOC**, conformado por:

1. **IQTEK SOLUTIONS, S.R.L.**, Sociedad de Responsabilidad Limitada, constituida de conformidad con las leyes de la República Dominicana, Registro Mercantil No. 87130SD, Registro Nacional de Contribuyentes (RNC) No. 1-30-87696-7, con domicilio social en la Calle Galá No. 8, sector Arroyo Hondo Viejo, Santo Domingo de Guzmán, Distrito Nacional;

2. **ULTRA TECH INC, S.A.**, persona jurídica constituida de conformidad con las leyes de la República de Panamá, inscrita en el Registro Público de Panamá, Folio 754130 (S) de la sección mercantil del registro público, al viernes 2 de diciembre de 2011, con domicilio social en , Calle 50 con Calle 56, Edificio F&F Tower, piso 47, oficina 47 C y D, Ciudad de Panamá, República de Panamá;

3. **GSI INTERNATIONAL, INC.**, sociedad de comercio de nacionalidad Panameña, organizada y existente de conformidad con las leyes de la República Dominicana, provista del Registro Nacional de Contribuyentes (RNC) No. 1-3014306-4, e inscrita en el Registro Mercantil con el No. 32067SD, y domicilio social en la Avenida 27 de febrero, esquina Tiradentes, Torre Empresarial Friusa, piso 8, suite 8B, La Esperilla;

4. **MÜHLBAUER ID SERVICES GMBH.**, sociedad de responsabilidad limitada constituida con arreglo a las leyes de la República Federal de Alemania, registrada en el Tribunal de Distrito de Ratisbona (Alemania) con el número HRB 9094, número de identificación a efectos del IVA VAT DE 813871380, con domicilio social en Josef-Mühlbauer-Platz 1, 93426 Roding, Alemania,

5. **VERIDOS GMBH**, sociedad de responsabilidad limitada, constituida según las leyes de Alemania, registrada en Juzgado Local de Charlottenburg, bajo el número HRB 155795 B, de Identificación Fiscal número 143/306/40066, con asiento social en Oranienstr. 91, 10969, Berlín, Alemania;

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

Por este medio de la presente **DECLARO BAJO LA FE DEL JURAMENTO** lo siguiente:

PRIMERO: Que la solución propuesta para las tarjetas de identificación de circuito integrado sin contacto cumple con el estándar ISO / IEC 14443.

SEGUNDO: Que la solución propuesta ha sido sometida a pruebas internas de calidad y seguridad, garantizando su fiabilidad y capacidad operativa en condiciones de uso exigentes, con un enfoque en la protección de la privacidad de los datos y la integridad del sistema.

La presente declaración se realiza para los fines requeridos para el Proceso de Licitación Pública Internacional No. **JCE-CCC-LPI-2024-0001**, en la ciudad de Santo Domingo de Guzmán, Distrito Nacional, capital de la República Dominicana, a los veinte (20) días del mes de febrero del año dos mil veinticinco (2025).

BERNARDO ANTONIO PÉREZ DIAZ
Representante del **CONSORCIO EMDOC**

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

Yo, **DRA. YILDA VERENISIA DE LEÓN**, Abogada - Notario Público de los del número del Distrito Nacional, autorizada mediante Matrícula No. 3004, **CERTIFICO Y DOY FE:** que por ante mí compareció el señor **BERNARDO ANTONIO PÉREZ DÍAZ**, de calidad que consta en el presente documento y a quien doy fe de conocer, quien me ha declarado que la firma puesta en el presente acto es la que acostumbra a utilizar en todos los actos de su vida. En la ciudad de Santo Domingo de Guzmán, Distrito Nacional, capital de la República Dominicana, a los veinte (20) días del mes de febrero del año dos mil veinticinco (2025).

YILDA VERENISIA DE LEÓN
Abogada – Notario Público

DRA. YILDA VERENISIA DE LEÓN
ABOGADA NOTARIO PÚBLICO DEL DISTRITO NACIONAL
MATRÍCULA No. 3004
Santo Domingo, R.D.

EMDOC
CONSORCIO

DECLARACIÓN JURADA

Quien suscribe, **BERNARDO ANTONIO PÉREZ DIAZ**, dominicano, mayor de edad, casado, portador de la Cédula de Identidad y Electoral No. 001-0196576-2, domiciliado y residente en esta ciudad de Santo Domingo de Guzmán, Distrito Nacional, capital de la República Dominicana, actuando en calidad de representante del **CONSORCIO EMDOC**, conformado por:

1. **IQTEK SOLUTIONS, S.R.L.**, Sociedad de Responsabilidad Limitada, constituida de conformidad con las leyes de la República Dominicana, Registro Mercantil No. 87130SD, Registro Nacional de Contribuyentes (RNC) No. 1-30-87696-7, con domicilio social en la Calle Galá No. 8, sector Arroyo Hondo Viejo, Santo Domingo de Guzmán, Distrito Nacional;

2. **ULTRA TECH INC, S.A.**, persona jurídica constituida de conformidad con las leyes de la República de Panamá, inscrita en el Registro Público de Panamá, Folio 754130 (S) de la sección mercantil del registro público, al viernes 2 de diciembre de 2011, con domicilio social en , Calle 50 con Calle 56, Edificio F&F Tower, piso 47, oficina 47 C y D, Ciudad de Panamá, República de Panamá;

3. **GSI INTERNATIONAL, INC.**, sociedad de comercio de nacionalidad Panameña, organizada y existente de conformidad con las leyes de la República Dominicana, provista del Registro Nacional de Contribuyentes (RNC) No. 1-3014306-4, e inscrita en el Registro Mercantil con el No. 32067SD, y domicilio social en la Avenida 27 de febrero, esquina Tiradentes, Torre Empresarial Friusa, piso 8, suite 8B, La Esperilla;

4. **MÜHLBAUER ID SERVICES GMBH.**, sociedad de responsabilidad limitada constituida con arreglo a las leyes de la República Federal de Alemania, registrada en el Tribunal de Distrito de Ratisbona (Alemania) con el número HRB 9094, número de identificación a efectos del IVA VAT DE 813871380, con domicilio social en Josef-Mühlbauer-Platz 1, 93426 Roding, Alemania,

5. **VERIDOS GMBH,** sociedad de responsabilidad limitada, constituida según las leyes de Alemania, registrada en Juzgado Local de Charlottenburg, bajo el número HRB 155795 B, de Identificación Fiscal número 143/306/40066, con asiento social en Oranienstr. 91, 10969, Berlín, Alemania;

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

Por este medio de la presente **DECLARO BAJO LA FE DEL JURAMENTO** lo siguiente:

PRIMERO: El **CONSORCIO EMDOC** se compromete a cumplir con el periodo de implementación en un plazo de veinte (20) semanas a partir de la firma del contrato adjudicado.

SEGUNDO: Durante dicho periodo, el **CONSORCIO EMDOC** se compromete a realizar todas las actividades relacionadas con la implantación y puesta en marcha del proyecto, de acuerdo con los plazos establecidos, incluyendo la entrega de productos, la realización de pruebas técnicas y la capacitación del personal de la JCE.

TERCERO: El **CONSORCIO EMDOC** garantiza la ejecución puntual y adecuada de todas las fases del proyecto dentro del plazo de veinte (20) semanas, y se compromete a realizar los ajustes necesarios conforme al desarrollo de las actividades, todo ello en cumplimiento con la cláusula 1.27.3 - Etapa 1: Implantación y puesta en marcha del proyecto del pliego de condiciones.

La presente declaración se realiza para los fines requeridos para el Proceso de Licitación Pública Internacional No. **JCE-CCC-LPI-2024-0001**, en la ciudad de Santo Domingo de Guzmán, Distrito Nacional, capital de la República Dominicana, a los veinte (20) días del mes de febrero del año dos mil veinticinco (2025).

BERNARDO ANTONIO PÉREZ DIAZ
Representante del **CONSORCIO EMDOC**

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

Yo, **DRA. YILDA VERENISIA DE LEÓN**, Abogada - Notario Público de los del número del Distrito Nacional, autorizada mediante Matrícula No. 3004, **CERTIFICO Y DOY FE:** que por ante mí compareció el señor **BERNARDO ANTONIO PÉREZ DÍAZ**, de calidad que consta en el presente documento y a quien doy fe de conocer, quien me ha declarado que la firma puesta en el presente acto es la que acostumbra a utilizar en todos los actos de su vida. En la ciudad de Santo Domingo de Guzmán, Distrito Nacional, capital de la República Dominicana, a los veinte (20) días del mes de febrero del año dos mil veinticinco (2025).

YILDA VERENISIA DE LEÓN
Abogada – Notario Público

REPÚBLICA DOMINICANA · NOTARÍA PÚBLICA DE LOS DEL NÚMERO DEL DISTRITO NACIONAL · Santo Domingo, R.D.

EMDOC
CONSORCIO

Plantilla (Matriz)

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

JCE-CCC-LPI-2024-0001

Se debe de rellenar el apartado cumple y no cumple, con la pagina del oferente donde lo cumple, así como comentarios adicionales si procede

Número		Entregado/No Entregado	Página del oferente	¿Subsanable?	Comentarios
1	DOCUMENTOS DE ACREDITACION PERSONAS JURIDICAS NACIONALES				
1.1	Comprobante de pago para cubrir gastos administrativos (Si aplica). Numeral 3.1.3 del Pliego	Si	"Acreditaciones y Solvencia", Carpeta 1, Iqtek Solutions SRL, pestaña 8, pg. 33. GSI International Inc, pestaña 26, pg. 213-214	SI	"Acreditaciones y Solvencia", Carpeta 1, Iqtek Solutions SRL, pestaña 8, pg. 33. GSI International Inc, pestaña 26, pg. 213-214
1.2	Carta de presentación de la empresa oferente. Numeral3.1.3 del Pliego	Si	"Acreditaciones y Solvencia", Carpeta 1, Iqtek Solutions SRL: pestaña 9, pgs 34-36. GSI International Inc, pestaña 27, pg. 215-216	SI	"Acreditaciones y Solvencia", Carpeta 1, Iqtek Solutions SRL: pestaña 9, pgs 34-36. GSI International Inc, pestaña 27, pg. 215-216
1.3	Copia del Registro Nacional del Contribuyente (RNC). Numeral 3.1.3 del Pliego	Si	"Acreditaciones y Solvencia", Carpeta 1, Iqtek Solutions SRL: pestaña 10, pgs 37-38. GSI International Inc, pestaña 28, pg. 217-218	SI	"Acreditaciones y Solvencia", Carpeta 1, Iqtek Solutions SRL: pestaña 10, pgs 37-38. GSI International Inc, pestaña 28, pg. 217-218
1.4	Registro Proveedores del Estado. Numeral 3.1.3 del Pliego	Si	"Acreditaciones y Solvencia", Carpeta 1, Iqtek Solutions SRL: pestaña 11, pgs 39-42. GSI International Inc, pestaña 29, pg. 217-220	SI	"Acreditaciones y Solvencia", Carpeta 1, Iqtek Solutions SRL: pestaña 11, pgs 39-42. GSI International Inc, pestaña 29, pg. 217-220
1.5	Copia de Cédula de Identidad y Electoral de la (s) persona (s) con poderes otorgados para suscribir el contrato de adjudicación. Numeral 3.1.3 del Pliego	Si	"Acreditaciones y Solvencia", Carpeta 1, Iqtek Solutions SRL: pestaña 12, pgs 43-45. GSI International Inc, pestaña 30, pg. 222-223	SI	"Acreditaciones y Solvencia", Carpeta 1, Iqtek Solutions SRL: pestaña 12, pgs 43-45. GSI International Inc, pestaña 30, pg. 222-223
1.6	Registro Mercantil (actualizado). Numeral 3.1.3 del Pliego	Si	"Acreditaciones y Solvencia", Carpeta 1, Iqtek Solutions SRL: pestaña 13, pgs 46-52. GSI International Inc, pestaña 31, pg. 224-230	SI	"Acreditaciones y Solvencia", Carpeta 1, Iqtek Solutions SRL: pestaña 13, pgs 46-52. GSI International Inc, pestaña 31, pg. 224-230
1.7	Carta del concesionario, casa matriz o distribuidor principal, indicando que el proponente es un suplidor autorizado de la marca ofertada y certificando que en caso de que el Proponente resulte adjudicatario, la firma asume el compromiso de suplir a éste; los materiales o servicios adjudicados. Numeral 3.1.3 del Pliego	Si	"Acreditaciones y Solvencia", Carpeta 1, Iqtek Solutions SRL: pestaña 14, pgs 53-57. GSI International Inc, pestaña 1-1, pg. 231-232	SI	"Acreditaciones y Solvencia", Carpeta 1, Iqtek Solutions SRL: pestaña 14, pgs 53-57. GSI International Inc, pestaña 1-1, pg. 231-232
1.8	Carta del concesionario, casa matriz, fabricante o distribuidor principal, en la que detalle las empresas o instituciones públicas del Estado para las cuales haya fabricado materiales similares a los requeridos mediante la presente licitación. Numeral 3.1.3 del Pliego	Si	Se incluyen cartas de fabricante Muhlbauer pagina 675.	SI	Se incluyen cartas de fabricante Muhlbauer pagina 575.
1.9	Copia de los Estatutos Sociales, debidamente registrados en la Cámara de Comercio, certificados como conforme a su original por el secretario, el presidente y/o el gerente de la compañía o por la persona con calidad para hacerlo y sellado con el sello social de la compañía. Numeral 3.1.3 del Pliego	Si	"Acreditaciones y Solvencia", Carpeta 1, Iqtek Solutions SRL: pestaña 15, pgs 58-78. GSI International Inc, pestaña 1-2, pg. 233-275	SI	"Acreditaciones y Solvencia", Carpeta 1, Iqtek Solutions SRL: pestaña 15, pgs 58-78. GSI International Inc, pestaña 1-2, pg. 233-275
1.10	Lista de la composición accionaria actualizada, debidamente registrada en la Cámara de Comercio, certificada como conforme a su original por el secretario, el Presidente y/o el gerente de la compañía y con el sello social. Numeral 3.1.3 del Pliego	Si	"Acreditaciones y Solvencia", Carpeta 1, Iqtek Solutions SRL: pestaña 16, pgs 79-81. GSI International Inc, pestaña 1-3, pg. 276-279	SI	"Acreditaciones y Solvencia", Carpeta 1, Iqtek Solutions SRL: pestaña 16, pgs 79-81. GSI International Inc, pestaña 1-3, pg. 276-279
1.11	Estados Financieros de los últimos tres (3) períodos fiscales, certificados por un Contador Público Autorizado, avalado con copia del IR-2 de esos últimos tres (3) períodos fiscales, incluyendo la entrega certificada con el soporte correspondiente y/o el código de envío electrónico recibido. Las hojas financieras auditadas deben presentarse según la plantilla facilitada en el Anexo 8. Todos los datos financieros (en la plantilla) deben expresarse en Dólares Estadounidenses (USD). Numeral 3.1.3 del Pliego.	Si	"Acreditaciones y Solvencia", Carpeta 1, Iqtek Solutions SRL: pestañas 18-19, pgs 82-192. Plantilla: pestaña24, pgs 209-211. GSI International Inc, pestañas 1-(4-5), pg. 280-410. Plantilla: pestaña11, pgs 426-427.	SI	"Acreditaciones y Solvencia", Carpeta 1, Iqtek Solutions SRL: pestañas 18-19, pgs 82-192. Plantilla: pestaña24, pgs 209-211. GSI International Inc, pestañas 1-(4-5), pg. 280-410. Plantilla: pestaña11, pgs 426-427.
1.12	Poder de representación otorgado ante Notario Público, en caso de que proceda. Cuando la empresa oferente esté representada por su Presidente o por algún directivo, y siempre y cuando los Estatutos Sociales le otorguen el poder de representación de la sociedad, no será necesario este requerimiento. Numeral 3.1.3 del Pliego	Si	"Acreditaciones y Solvencia", Carpeta 1, Iqtek Solutions SRL: pestaña 20, pgs 193-195. GSI International Inc, pestaña 1-6, pg. 411-417	SI	"Acreditaciones y Solvencia", Carpeta 1, Iqtek Solutions SRL: pestaña 20, pgs 193-195. GSI International Inc, pestaña 1-6, pg. 411-417

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

1.13	Certificación donde se haga constar que está al día en el pago de sus obligaciones fiscales (original). Numeral 3.1.3 del Pliego	Si	"Acreditaciones y Solvencia", Carpeta 1, Iqtek Solutions SRL: pestaña 21, pgs 198-199. GSI International Inc, pestaña 1-7, pg. 418-419	SI	"Acreditaciones y Solvencia", Carpeta 1, Iqtek Solutions SRL: pestaña 21, pgs 198-199. GSI International Inc, pestaña 1-7, pg. 418-419
1.14	Certificación donde se haga constar que está al día en el pago de la Seguridad Social (original). Numeral 3.1.3 del Pliego	Si	"Acreditaciones y Solvencia", Carpeta 1, Iqtek Solutions SRL: pestaña 22, pgs 200-201. GSI International Inc, pestaña 1-8, pg. 420-421	SI	"Acreditaciones y Solvencia", Carpeta 1, Iqtek Solutions SRL: pestaña 22, pgs 200-201. GSI International Inc, pestaña 1-8, pg. 420-421
1.15	Declaración Jurada del solicitante ante un notario público, debidamente legalizada en la Procuraduría General de la República Dominicana, en la que manifieste que no se encuentra dentro de las prohibiciones establecidas en el Artículo 14 de la Ley 340-06, sobre Compras y Contrataciones Públicas. (Usar modelo denominado FL-06 que se encuentra anexo al Pliego). Numeral 3.1.3 del Pliego	Si	"Acreditaciones y Solvencia", Carpeta 1, Iqtek Solutions SRL: pestaña 23, pgs 202-203. GSI International Inc, pestaña 1-9, pg. 422-423	SI	"Acreditaciones y Solvencia", Carpeta 1, Iqtek Solutions SRL: pestaña 23, pgs 202-203. GSI International Inc, pestaña 1-9, pg. 422-423
1.16	Cartas de referencias bancarias y/o entidades financieras, dirigidas a la Junta Central Electoral, que demuestren solvencia y respaldo económico y/o que certifiquen que posee línea de crédito que pueda solventar al menos el monto de Dos Millones de Dólares Estadounidenses (USD$2,000,000.00), o su equivalente en pesos o euros.3.1.3 del pliego. Se sugiere que al menos uno (1) de los miembros que componen el grupo del consorcio cumpla con este requisito. Numeral 5.4.1 del Pliego.	Si	"Acreditaciones y Solvencia", Carpeta 1, Iqtek Solutions SRL: pestaña 24, pgs 204-208.D28	SI	"Acreditaciones y Solvencia", Carpeta 1, Iqtek Solutions SRL: pestaña 24, pgs 204-208.D28
1.17	El oferente deberá proporcionar un mínimo de diez (10) muestras de las tarjetas junto con la propuesta técnica (estas muestras son adicionales a las requeridas para la prueba de concepto). Las muestras deben ser capaces de representar la personalización de las cédulas electrónicas y los detalles de las características que el proveedor propone, y éstas deben explicarse claramente. Junto con las muestras, el proveedor deberá presentar informes de pruebas independientes de acuerdo a la norma ISO 18745. Numeral 3.1.3 del Pliego	Si	Nuestra propuesta contempla la entrega de las diez (10) muestras de tarjetas, ver detalle (Carpeta negra de 3 argollas). De igual forma se incluyen las pruebas de laboratorio independiente	NO	Nuestra propuesta contempla la entrega de las diez (10) muestras de tarjetas, ver detalle (Carpeta negra de 3 argollas). De igual forma se incluyen las pruebas de laboratorio independiente
1.18	Las empresas que actúen como Consorcio deben depositar un acuerdo bajo firma privada de constitución de consorcio, que haga a sus integrantes corresponsables de las acciones de este, incluyendo su objeto, las obligaciones de las partes, su porcentaje de participación y su relación con el órgano licitante. El documento debe ser debidamente notariado y legalizado. Numeral 3.1.5 del Pliego	Si	Carpeta 1, "Acreditaciones y Solvencia", pestaña 1, pgs 15-17	SI	Carpeta 1, "Acreditaciones y Solvencia", pestaña 1, pgs 15-17
2	DOCUMENTOS DE ACREDITACION PERSONAS JURIDICAS EXTRANJERAS				
2.1	Comprobante de pago para cubrir gastos administrativos (Si aplica). Numeral 3.1.4 del Pliego	Si	IQTek pagina 32 y GSI International INC. pagina 213	SI	IQTek pagina 32 y GSI International INC. pagina 213
2.2	Carta de presentación de la empresa oferente. Numeral 3.1.4 del Pliego	Si	"Acreditaciones y Solvencia", Carpeta 1, Ultra Tech Inc. SA, pestaña 2-12, pg. 429-431.	SI	"Acreditaciones y Solvencia", Carpeta 1, Ultra Tech Inc. SA, pestaña 2-12, pg. 429-431.
2.3	Copia del pasaporte o documento de identificación válido de la persona con poderes otorgados para suscribir el contrato de adjudicación. Numeral 3.1.4 del Pliego	Si	"Acreditaciones y Solvencia", Carpeta 1, Ultra Tech Inc. SA, pestaña 2-15, pg. 437-441.	SI	"Acreditaciones y Solvencia", Carpeta 1, Ultra Tech Inc. SA, pestaña 2-15, pg. 437-441.
2.4	Carta del concesionario, casa matriz o distribuidor principal, indicando que el proponente es un suplidor autorizado de la marca ofertada y certificando que en caso de que el Proponente resulte adjudicatario, la firma asume el compromiso de suplir a éste; los materiales o servicios adjudicados. Numeral 3.1.4 del Pliego	Si	"Acreditaciones y Solvencia", Carpeta 1, Ultra Tech Inc. SA, pestaña 2-17, pg. 446-447.	SI	"Acreditaciones y Solvencia", Carpeta 1, Ultra Tech Inc. SA, pestaña 2-17, pg. 446-447.
2.5	Carta del concesionario, casa matriz, fabricante o distribuidor principal, en la que detalle las empresas o instituciones de gobiernos para las cuales haya fabricado materiales similares a los requeridos mediante la presente licitación. Numeral 3.1.4 del Pliego	Si	Se incluyen cartas de fabricante Muhlbauer pagina 675 y Veridos pagina 944	SI	Se incluyen cartas de fabricante Muhlbauer pagina 675 y Veridos pagina 944
2.6	Certificación de pago de la Tesorería de la Seguridad Social -TSS- (En el caso de una persona extranjera, este requisito sólo aplicará cuando dicha empresa se encuentre domiciliada y/o legalmente representada en la República Dominicana). Numeral 3.1.4 del Pliego	Si	"Acreditaciones y Solvencia", Carpeta 1, Ultra Tech Inc. SA, pestaña 2-24, pg. 602-605.	SI	"Acreditaciones y Solvencia", Carpeta 1, Ultra Tech Inc. SA, pestaña 2-24, pg. 602-605.
2.7	Constancia de inscripción en el Registro de Proveedores del Estado (RPE). En el caso de una empresa extranjera, no necesitará estar registrada en el RPE, salvo el caso de que se encuentre domiciliada en la Rep. Dom. Sin embargo, si resulta adjudicataria, previa suscripción del contrato, deberá obtener y depositar el registro correspondiente. Numeral 3.1.4 del Pliego	Si	Carpeta 1, "Acreditaciones y Solvencia", EMDOC: pestaña 4, pgs 21-22. Ultra Tech Inc. SA, pestaña 2-14, pg. 435-436	SI	Carpeta 1, "Acreditaciones y Solvencia", EMDOC: pestaña 4, pgs 21-22. Ultra Tech Inc. SA, pestaña 2-14, pg. 435-436

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

2.8	La empresa extranjera que resulte adjudicataria deberá solicitar su Registro de Proveedores del Estado (RPE) en un plazo no mayor de diez (10) días hábiles a partir de la fecha de notificación de adjudicación. Pasado este plazo sin que se realice dicha inscripción quedará excluida del proceso sin más trámite. Numeral 3.1.4 del Pliego	Si	La empresa Mulbahuer tiene un RPE provisional en la pagina 628 y Veridos en la pagina 915.	SI	La empresa Mulbahuer tiene un RPE provisional en la pagina 628 y Veridos en la pagina 915.
2.9	Declaración Jurada del solicitante ante un notario público, debidamente legalizada en la Procuraduría General de la República Dominicana, en la que manifieste que no se encuentra dentro de las prohibiciones establecidas en el Artículo 14 de la Ley 340-06, sobre Compras y Contrataciones Públicas. (Usar modelo denominado **FL-06** que se encuentra anexo al Pliego). Numeral 3.1.4 del Pliego	Si	IQTek pagina 202 y GSI International INC. pagina 422, Mulbahuer pagina 880, Veridos pagina 1125.	SI	IQTek pagina 202 y GSI International INC. pagina 422, Mulbahuer pagina 880, Veridos pagina 1125.
2.10	Poder de representación otorgado ante Notario Público, en caso de que proceda. En caso de que la firma que otorgue el poder no esté establecida en el país, el Poder de Representación deberá ser certificado ante el consulado acreditado por el Estado Dominicano en el país de emisión y legalizado en el Ministerio de Relaciones Exteriores de la República Dominicana (MIREX). Numeral 3.1.4 del Pliego	Si	Poder de representacion pagina 15	SI	Poder de representacion pagina 15
2.11	Todo poder que hubiese sido otorgado en un idioma que no sea el español; deberá de ser traducido por un intérprete judicial en la República Dominicana, en cuyo caso la firma de traducción deberá estar legalizada en la Procuraduría General de República. En caso de que la empresa Oferente esté representada por su Presidente o por uno de sus directivos, siempre y cuando los Estatutos Sociales le otorguen el Poder de Representación de la sociedad, no será necesario presentar este requerimiento. Numeral 3.1.4 del Pliego	Si	Se incluye el poder debidamente traducido pagina 837	SI	Se incluye el poder debidamente traducido pagina 837
2.12	Documentación pertinente que demuestre la legalidad de la constitución de la empresa en su país de origen. Deberán depositar junto a los documentos constitutivos exigidos por el país de origen, un certificado de "Good Standing", o su equivalente en el país del que se trate, que es el certificado de existencia de la compañía, expedido por la entidad gubernamental o Estatal respectiva. Dicho documento deberá contener las legalizaciones correspondientes. Numeral 3.1.4 del Pliego	Si	Ultratech pagina 443, Muhlbauer pagina 642, IQTEK pagina 47, GSI Int. Inc. pagina 225 , Veridos pagina 920	SI	Ultratech pagina 443, Muhlbauer pagina 642, IQTEK pagina 47, GSI Int. Inc. pagina 225 , Veridos pagina 920
2.13	Certificación actualizada y legible del organismo, que, en el país de origen de la empresa, sea el que determine que la misma se encuentra al día con sus obligaciones fiscales. Numeral 3.1.4 del Pliego	Si	Ultratech pagina 599 , Muhlbauer pagina 861, IQTEK pagina 199, GSI Int. Inc. pagina 419 , Veridos pagina 1114	SI	Ultratech pagina 599 , Muhlbauer pagina 861, IQTEK pagina 199, GSI Int. Inc. pagina 419 , Veridos pagina 1114
2.14	Copia certificada del equivalente físico o electrónico al formulario IR-2 de la DGII (Dirección General de Impuestos Internos), o su equivalente, de los últimos tres (3) períodos fiscales, donde quede constancia oficial de la valoración efectiva de los aportes fiscales en su país de origen. Las hojas financieras auditadas deben presentarse según la plantilla facilitada en el Anexo 9. Todos los datos financieros (en la plantilla) deben expresarse en Dólares Estadounidenses (USD). Numeral 3.1.4 del Pliego	Si	GSI Int. Inc. pagina 347 a 410. IQTEK: pagina 139-192. Ultra pagina 582-592	SI	GSI Int. Inc. pagina 347 a 410. IQTEK: pagina 139-192. Ultra pagina 582-592
2.15	Cartas de referencias bancarias y/o entidades financieras, dirigidas a la Junta Central Electoral, que demuestren solvencia y respaldo económico y/o que certifiquen que posee línea de crédito que pueda solventar al menos el monto de USD$2.000.000.00 (o su equivalente en pesos o euros). 3.1.4 del pliego. Se sugiere que al menos uno (1) de los miembros que componen el grupo del consorcio cumpla con este requisito o en su conjunto. Numeral 5.4.1 del pliego	Si	IQTEK pagina 205 a la 208. GSI Int. Inc. pagina 425, Ultratech pagina 610,Muhlbauer pagina 823, Veridos pagina 1128.	SI	IQTEK pagina 205 a la 208. GSI Int. Inc. pagina 425, Ultratech pagina 610,Muhlbauer pagina 823, Veridos pagina 1128.
2.16	El oferente deberá proporcionar un mínimo de diez (10) muestras originales de las tarjetas junto con la propuesta técnica. Las muestras deben ser capaces de representar la personalización de las cédulas electrónicas y los detalles de las características de seguridad que el proveedor propone, y éstas deben explicarse claramente. Junto con las muestras, el proveedor deberá presentar informes de pruebas independientes de acuerdo con la norma ISO 18745. Numeral 3.1.4 del Pliego	Si	Nuestra propuesta contempla la entrega de las diez (10) muestras de tarjetas, ver detalle (Carpeta negra de 3 argollas). De igual forma se incluyen las pruebas de laboratorio independiente	NO	Nuestra propuesta contempla la entrega de las diez (10) muestras de tarjetas, ver detalle (Carpeta negra de 3 argollas). De igual forma se incluyen las pruebas de laboratorio independiente
2.17	Las empresas que actúen como Consorcio deben depositar un acuerdo bajo firma privada de constitución de consorcio, que haga a sus integrantes corresponsables de las acciones de este, incluyendo su objeto, las obligaciones de las partes, su porcentaje de participación y su relación con el órgano licitante. El documento debe ser debidamente notariado y legalizado. Numeral 3.1.4 del Pliego	Si	Carpeta 1, "Acreditaciones y Solvencia", pestaña 1, pgs 15-17	SI	Carpeta 1, "Acreditaciones y Solvencia", pestaña 1, pgs 15-17
3	**DOCUMENTOS TECNICOS**				
3.1	**Resumen ejecutivo.** Numeral 3.1.6.1 del Pliego				
3.1.1	Presentación de la empresa o consorcio.	Si	465-1 a 467	SI	Carta de Presentación
3.1.2	Visión del proyecto sugerencias y recomendaciones.	Si	467-1 a 469	SI	Visioón del Proyecto

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

3.1.3	Curriculum del líder del proyecto o jefe de proyecto, que debe tener como mínimo 5 años de experiencia en uno o varios proyectos de identificación de tarjetas de policarbonato en instituciones públicas, tener certificado PMP, PRINCE2 o similar, así como conocimientos ITIL. Para acreditar dicha experiencia, el oferente debe aportar el Curriculum Vitae del candidato, así como detallar las experiencias de la persona propuesta en una de las empresas del consorcio.	Si	470-481	SI	Curriculum del líder del proyecto o jefe de proyecto
3.1.4	Curriculum del personal técnico certificado en tecnología de impresión de tarjetas de identidad localmente durante la vigencia del contrato para supervisión de la calidad de la impresión en todos los centros de impresión de cédulas. Se deben incluir las certificaciones correspondientes.Para acreditar dicha experiencia, el oferente debe aportar el Curriculum Vitae del candidato, así como detallar las experiencias de la persona propuesta en una de las empresas del consorcio.	Si	482-585	SI	Curriculum del personal técnico certificado en tecnología de impresión de tarjetas de identidad
3.1.5	Curriculum del personal técnico en campo (a nivel nacional) con experiencia en la producción de documentos de identidad nacionales mediante modelo descentralizado de impresión, ofreciendo servicios de instalación, soporte y mantenimiento a la infraestructura de impresión durante los años de garantía de los equipos. Para acreditar dicha experiencia, el oferente debe aportar el Curriculum Vitae del candidato, así como detallar las experiencias de la persona propuesta en una de las empresas del consorcio.	Si	482-585	SI	Curriculum del personal técnico certificado en tecnología de impresión de tarjetas de identidad
3.2	**Requisitos de experiencia (OBLIGATORIOS). TODOS LOS DOCUMENTOS PRESENTADOS PARA ACREDITAR LA EXPERIENCIA, DEBE APARECER LOS DATOS DE LA INSTITUCIÓN PUBLICA, ASI COMO EL NOMBRE DE LA PERSONA A CARGO DE LA INSTITUCIÓN, CARGO, DIRECCIÓN FISICA Y ELECTRONICA, TELEFONO DIRECTO E EMAIL PARA PODER VALIDAR LA REFERENCIA. Numeral 3.1.6.2 del Pliego**				
3.2.1	Al menos una (1) experiencia en un proyecto, en el cual el oferente haya llevado a cabo el suministro de impresoras de documentos de identidad de policarbonato electrónicos, incluyendo la instalación y el mantenimiento.Solo serán válidos contratos (en vigor o terminados) dentro de los últimos 5 años a partir de la fecha de presentación de la propuesta y a nivel de institución pública.	Si	791-793 794-802	SI	Expeeriencia y Suministro de Impresoras de documentos de identidad de policarbonato electrónicos - Carta de Ministerio de Gobernación y Policía - Montenegro Ministry of Interior (ver traducción y apostilla)
3.2.2	Al menos una (1) experiencia en un proyecto, en el cual el oferente haya llevado a cabo un suministro de tarjetas de identidad electrónicas de policarbonato. Sólo serán válidos contratos (en vigor o terminados) dentro de los últimos 5 años a partir de la fecha de presentación de la propuesta y a nivel de institución pública	Si	803-809	SI	Experiencia en proyecto de suministros de tarjstas de identidad electrónicas de policarbonato - Ministerio de Gobernación y Policía - RENAP
3.2.3	Al menos una (1) experiencia, en el cual el oferente haya implementado un proyecto de transición de documentos de identificación mecánicos (sin electrónica) a documentos de identificación electrónicos. Solo serán válidos contratos (en vigor o terminados) dentro de los últimos 5 años a partir de la fecha de presentación de la propuesta.	Si	810-816 817-836	SI	Experiencia en proyecto de suministro de tarjetas de identidad electrónicas de policarbonato de transición de documentos de identificación mecánicos (sin eletrónica) a documento de identificación electrónicos. - Ministerio de Gobernación y Justicia - Ministerio De Interior Gabinete Do Minister)
3.2.4	Al menos una (1) experiencia, en el cual el oferente haya realzado una integración de sistemas, en un proyecto de identificación electrónica. Solo serán válidos contratos (en vigor o terminados) dentro de los últimos 5 años a partir de la fecha de presentación de la propuesta. Solo serán válidos contratos (en vigor o terminados) dentro de los últimos 5 años a partir de la fecha de presentación de la propuesta.	Si	837-843	SI	Experiencia en integración de sistemas, en un proyecto de identificación electrónica
3.3	**Requisitos de experiencia (NO OBLIGATORIOS) 3.1.6.3 del pliego**				
3.3.1	Más de una (1) experiencia, en distintos clientes y países, en cédulas digital o identidades móviles (Mobile ID). Solo serán válidos contratos de al menos proyectos de 100,000 cédulas en total, dentro de los últimos 5 años a partir de la fecha de presentación de la propuesta. Al menos una de las referencias debe ser ISO 18013-5.	Si	845-848	SI	Registro Nacional de las Personas Naturales

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

3.3.2	Al menos una (1) experiencia de haber operado un proyecto de impresión de soluciones de identificación a nivel de gobierno con el suministro y mantenimiento de al menos doscientas (200) impresoras distribuidas nacional e internacional (fuera del país).	Si	852-891	SI	Experiencia en República Dominicana en proyectos de mantenimiento de tecnología en gobierno con al menos cinco (5) años de experiencia: Hacienda - Gobierno de República Dominicana Ref. JCE-CCC-LPI-2024-0001 - Contrato de Compras de Bienes y Servicios Conexos Núm MH-2021-000029 - Contrato de Ejecución de Servicios núm. MH-2021-000005
3.3.3	Al menos una (1) experiencia en República Dominicana en proyectos de mantenimiento de tecnología en gobierno con al menos cinco (5) años de experiencia.	Si	791-801	SI	Experiencia en suministro de impresoras de documentos de identidad de policarbonato electrónicos: - Junta Central Electoral (JCE) - Montenegro Ministry of Interior
4	PROPUESTAS Y ANEXOS				
4.1	Propuesta Técnica (1 original y 3 copias)	Si	Cumple	NO	8. DOCUMENTOS TÉCNICOS
4.2	Propuesta Técnica en formato digital	Si	Cumple	SI	
4.3	FL-05 Presentación de Oferta Económica (Sobre B). Capítulo VIII del Pliego	Si	Cumple	NO	
4.4	FL-01 Formulario de inscripción. Capítulo VIII del Pliego	Si	Comprobante de pago GSI recibo 213 y IQTEK 32	Si	
4.5	FL-02 Formulario de Presentación de Ofertas. Capítulo VIII del Pliego	Si	"Acreditaciones y Solvencia", Carpeta 1, pestaña 5, pgs 23-26	Si	
4.6	FL-03 Carta de designación o sustitución de Agentes Autorizados. Capítulo VIII del Pliego	Si	"Acreditaciones y Solvencia", Carpeta 1, pestaña 6, pg. 27	Si	
4.7	FL-04 Carta de aceptación de designación como Agente Autorizado. Capítulo VIII del Pliego	Si	"Acreditaciones y Solvencia", Carpeta 1, pestaña 7, pgs. 29-30	Si	

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

JCE-CCC-LPI-2024-0001				
Se debe de rellenar el apartado cumple y no cumple, con la pagina del oferente donde lo cumple, asi como comentarios adicionales si procede				
Número		**Cumple/No Cumple**	**Página del oferente**	Comentarios
1	**REQUERIMIENTOS GENERALES**			
1.1	Deberán formalizar su inscripción (CON CARÁCTER OBLIGATORIO) mediante el llenado y presentación del Formulario FL-01 (Inscripción de Oferente), el cual se encuentra anexo al presente Pliego de Condiciones, y se podrá retirar en las oficinas del Comité de Compras y Contrataciones o descargarse de la página web de la Junta Central Electoral o del Portal Transaccional de la Dirección General de Contrataciones Públicas. El plazo para inscripción o registro de oferentes vence a las 4 horas de la tarde (4:00 P.M.) del día 17 de mayo del 2024. Capítulo VIII del Pliego. **(Repetido 4.4 de Credenciales y Propuestas).**	Si	Comprobante de pago GSI recibo 213 y IQTEK 32	Comprobante de pago GSI recibo 213 y IQTEK 32
1.2	El consorcio debe licitar como una sola entidad. Por lo tanto, los miembros del consorcio deben elegir al líder del consorcio para que lo represente. Numeral 5.4.1 del Pliego	Si	Acuerdo intencion de consorcio pagina 3-14	Acuerdo intencion de consorcio pagina 3-14
1.3	Ningún oferente (de tarjetas, de impresoras, de cédula digital, de ABIS) podrá presentar más de una Oferta para el Proyecto. Un oferente que licite individualmente o como miembro de un consorcio no tendrá derecho a presentar otra oferta ni individualmente ni como miembro de ningún Consorcio. Esta restricción no se aplica a los proveedores de materiales o equipos tales como equipos de infraestructura, dispositivos o consumibles. PARA ACREDITAR LA ELEGILIBILIDAD, EL OFERENTE DEBERÁ HACER UNA CARTA JURADA ASEGURANDO QUE SUS MIEMBROS SOLO PARTICIPA EN UN CONSORCIO EN ESTA LICITACIÓN. Numeral 5.4.1 del Pliego	Si	Refierase a la Seccion de Cartas Juradas- Sobre A de Documentos Tecnicos	Refierase a la Seccion de Cartas Juradas- Sobre A de Documentos Tecnicos
1.4	Al presentar su oferta mediante el Formulario FL-02 (Anexo 2), el oferente acepta el contenido del presente pliego y sus modificaciones posteriores incluyendo las respuestas a las preguntas durante el proceso de licitación. Numeral 5.4.1 del Pliego. **(Repetido 4.5 de Credenciales y Propuestas).**	Si	Pagina -24-25	Pagina -24-25
1.5	El oferente deberá presentar cartas de referencias bancarias y/o entidades financieras, dirigidas a la Junta Central Electoral, que demuestren solvencia y respaldo económico y/o que certifiquen que posee línea de crédito que pueda solventar al menos el monto de USD$2,000,000.00 (o su equivalente en pesos o euros). Se sugiere que al menos uno (1) de los miembros que componen el grupo del consorcio cumpla con este requisito. Numeral 5.4.1 del Pliego. **(Repetido 1.16 y 2.15 de Credenciales y Propuestas).**	Si	IQTEK pagina 205 a la 208. GSI Int. Inc. pagina 425. Ultratech pagina 610,Muhlbauer pagina 823, Veridos pagina 1128.	IQTEK pagina 205 a la 208. GSI Int. Inc. pagina 425. Ultratech pagina 610,Muhlbauer pagina 823, Veridos pagina 1128.
1.6	El oferente deberá presentar los Estados Financieros de los últimos tres (3) periodos fiscales, certificados por un Contador Público Autorizado, avalado con copia del IR-2 de esos últimos tres (3) períodos fiscales, incluyendo la entrega certificada con el soporte correspondiente y/o el código de envío electrónico recibido. Numeral 5.4.1 del Pliego. **(Repetido 1.11 y 2.14 de Credenciales y Propuestas)**.	Si	Estados Financieros IR-2IQTEK: de pagina 82 -192. GSI de la pagina 280-410, UltraTEch 490 -592. Muhlbauer pag.712-836,Veridos pag. 991- 1104	Estados Financieros IR-2IQTEK: de pagina 82 -192. GSI de la pagina 280-410, UltraTEch 490 -592. Muhlbauer pag.712-836,Veridos pag. 991- 1104

CONSORCIO EMDOC
EMDOC CONSORCIO
Santo Domingo, R.D.

1.7	Las hojas financieras auditadas deben presentarse según la plantilla facilitada (Anexo 8). Numeral 5.4.1 del Pliego. **(Repetido 1.11 y 2.14 de Credenciales y Propuestas).**	Si	IQTEK pagina 210. GSI Int. Inc. pagina 427 , Ultratech pagina 614, Muhlbauer pagina 891,Veridos pagina 1137	IQTEK pagina 210. GSI Int. Inc. pagina 427 , Ultratech pagina 614, Muhlbauer pagina 891,Veridos pagina 1137
1.8	El plazo de validez de las ofertas será de ciento cincuenta (150) días a partir de la fecha límite. Numeral 5.4.1 del pliego	Si	Cumple	Cumple
1.9	El oferente deberá proporcionar un mínimo de diez (10) muestras originales de las tarjetas junto con la propuesta técnica. Las muestras deben ser capaces de representar la personalización de las cédulas electrónicas y los detalles de las características de seguridad que el proveedor propone, y éstas deben explicarse claramente. Junto con las muestras, el proveedor deberá presentar informes de pruebas independientes de acuerdo con la norma ISO 18745. Las tarjetas preimpresas a entregar pueden ser genéricas; sin embargo, es fundamental que demuestren, ya sea de manera individual o sumando características, todas y cada una de las especificaciones requeridas en el pliego de condiciones. En total las terjetas a entregar deberán evidenciar las especificaciones técnicas solicitadas. Sólo es necesario presentar documentos de laboratorio externo que acrediten que el oferente cumple con la norma ISO 18745 para cualquiera de sus productos fabricados. No específico para las muestras. Numeral 5.4.1 del Pliego. **(Repetido 1.17 y 2.16 de Credenciales y Propuestas).**	Si	Nuestra propuesta contempla la entrega de las diez (10) muestras de tarjetas, ver detalle (Carpeta negra de 3 argollas). De igual forma se incluyen las pruebas de laboratorio independiente	Nuestra propuesta contempla la entrega de las diez (10) muestras de tarjetas, ver detalle (Carpeta negra de 3 argollas). De igual forma se incluyen las pruebas de laboratorio independiente
1.10	Solvencia (Activo total / Pasivo total) del Consorcio debe ser mayor que >1. PARA ACREDITAR LA ELIGIBILIDAD , EL OFERENTE DEBERÁ REALIZAR UNA CARTA JURADA DICIENDO QUE SU SOLVENCIA ES MAYOR QUE UNO, ADJUNTANDO LOS ESTADOS FINANCIEROS DEL CONSORCIO Y RESALTANDO DE DONDE SE OBTIENEN LOS VALORES PARA REALIZAR DICHO CÁLCULO.	Si	Refierase a la Seccion de Cartas Juradas- Sobre A de Documentos Tecnicos	Se incluye Carta Jurada
1.11	Consorcio debe facturar (de media en los últimos 3 años) en su conjunto, al menos la totalidad del presupuesto de su propuesta total. PARA ACREDITAR EL REQUISITO, EL OFERENTE DEBE DE PRESENTAR CARTA JURADA ASEGURANDO QUE SU FACTURACION ES AL MENOS , LA TOTALIDAD DEL PRESUPUESTO DE SU OFERTA QUE SERÁ COMPROBADA EN EL SOBRE B.	Si	Refierase a la Seccion de Cartas Juradas- Sobre A de Documentos Tecnicos	Se incluye Carta Jurada
1.12	**Máximo** tiempo de implementación: 26 semanas.	Si	Cumple, ver mayores detalles en el plan del proyecto y cronograma pagina 789 A 789 L	Cumple, ver mayores detalles en el plan del proyecto y cronograma pagina 789 A 789 L
1.13	Impresora pesa menos de 80kg.	Si	60	ITEM II. MÁQUINAS DE IMPRESIÓN . Características técnicas
1.14	Impresora modular.	Si	58	Características Generales de la Máquina de Impresión
1.15	Que el proponente esté legalmente autorizado para realizar sus actividades comerciales en el país.	Si	Registro Mercnatil de GSI Int. Inc.pagina 225 y IQTEK pagina 46	

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

1.16	Que el oferente demuestre que tiene capacidad y experiencia para la entrega a tiempo y en las condiciones establecidas.	Si	El consorcio cuenta con capacidad y experiencia comprobada en la entrega a tiempo de acuerdo con lo solicitado en el pliego de cargos. Refierase a las cartas de experiencia obligatoria y No obligatorias pagina: 790-891	
1.17	Que cuenta con la estabilidad financiera suficiente para ejecutar satisfactoriamente la eventual adjudicación. De las empresas nacionales, se evaluarán los estados financieros auditados de los últimos tres (3) periodos fiscales y el **formulario IR-2** con sus respectivos anexos para determinar los Índices Financieros mínimos correspondientes. Para las empresas extranjeras, no se requiere los Estados Financieros, éstas deben presentar la plantilla financiera (Anexo 8) en dólares estadounidenses (USD), tiene que presentar copia certificada del equivalente físico o electrónico al formulario IR-2	Si	GSI Int. Inc. pagina 347 a 410. IQTEK: pagina 139-192. Ultra pagina 582-592	GSI Int. Inc. pagina 347 a 410. IQTEK: pagina 139-192. Ultra pagina 582-592
1.18	La experiencia del Mobile ID debe ser de alguna empresa del consorcio. PARA ACREDITAR LA ELIGIBILIDAD , EL OFERENTE DEBERÁ REALIZAR UNA CARTA JURADA DICIENDO CUAL DE SUS MIEMBROS TIENE UNA EXPERIENCIA EN CEDULA DIGITAL (MOBILE ID). Se aceptarán contratos de empresas miembros de un mismo grupo económico, siempre que se pueda demostrar que se trata de accionistas en común.	Si	Refierase a la pagina 846- 848	Se incluye Carta Jurada
2	**REQUERIMIENTOS DEL PROVEEDOR**			
2.1	Contar con la acreditación de la fábrica de pasaporte del certificado INTERGRAF ISO 14298:2013 o superior, a nivel gobierno en vigencia	Seleccionar	Ver certificacion de Muhlbauer de la pagina 587-594	
2.2	Tener el certificado ISO 27001 en vigencia del fabricante de la tarjeta. Numeral 5.4.1 del Pliego.	Seleccionar	Ver certificado Muhlbauer pag. 595 -605	
2.3	Tener el certificado ISO 14001 en vigencia del fabricante de la tarjeta. Numeral 5.4.1 del Pliego.	Seleccionar	Ver certificado Muhlbauer pag. 605-614	
2.4	Tener el certificado ISO 9001 en vigencia del fabricante de la tarjeta. Numeral 5.4.1 del Pliego.	Seleccionar	Ver certificado Muhlbauer pag. 605-614	
2.5	Tener el certificado ISO 50001 en vigencia, al menos una empresa del consorcio. Especificaciones Técnicas Generales del Pliego, págs. 14 y 15	Seleccionar	Ver certificado Muhlbauer pag. 615-634	
2.6	Tener el certificado CWA 15374:2018 En vigencia . Observacion del Grupo 4 respuestas 22: Con la presentación del certificado del fabricante de tarjeta de ISO14298 a nivel gubernamental no se hace necesario la presentación del certificado CWA15374. Quien aporte dicho certificado debe estar dentro del consorcio. Con la presentación del certificado del fabricante de tarjeta de ISO14298 (2.1 arriba)a nivel gubernamental no se hace necesario la presentación del certificado CWA15374. Quien aporte dicho certificado debe estar dentro del consorcio. Con la presentación del certificado del fabricante de tarjeta de ISO14298 a nivel gubernamental no se hace necesario la presentación del certificado CWA15374. Quien aporte dicho certificado debe estar dentro del consorcio. Especificaciones Técnicas Generales del Pliego, pág. 14	Seleccionar	Ver certificado Muhlbauer pag. 635-641	

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

2.7	ISO 15408: PKI Compatible con ICAO para establecer un SOD activado en los datos del chip. Especificaciones Técnicas Generales del Pliego, págs. 14 y 15	Seleccionar	Ver Carta Jurada de ISO 15408 en la cual se certifica que nuestra solucion de PKI es compatible con ICAO para establecer un SOD activado en los datos del chip.	
2.8	ISO / IEC 14443 Tarjetas de identificación de circuito integrado sin contacto. ITEM I, numeral I .3 del Pliego, pág. 16	Seleccionar	Ver Carta Jurada de ISO /IECC 14443 en la cual se certifica que las tarjetas de identificacion de circuito integrado sin contacto.	
3	**OTROS REQUERIMIENTOS TECNICOS**			
3.1	Cronograma de trabajo: El oferente deberá presentar un plan de trabajo detallado que cubra las tres (3) etapas del proyecto. (ver numeral 1.27.2).	Si	789-A a 789-F 789G a 789I	Ver Detalle del Cronograma Cumplimiento Ver Cronograma
3.2	Etapa 1: Implantación y puesta en marcha del proyecto En esta etapa, que durará máximo veintiséis (26) semanas a partir de la firma del contrato.	Si	789-D 789G a 789-I	Ver Detalle del Cronograma Cumplimiento, las actividades listadas se cumplen hasta la semana 20, punto 6. Realizar pruebas piloto de solución digital de la tarjeta CD (Mobile ID) antes veintiséis (26) semanas, incluyen el desarrollo de una app para la JCE (siempre que la JCE cumpla con sus dependencias a tiempo), página 2 Ver Cronograma
3.3	Etapa 2: Durará máximo 12 meses a partir de la finalización de la etapa 1	Si	789-C a 789-D 789G a 789-I	Ver Detalle del Cronograma Cumplimiento, Etapa 2: Máximo 12 meses a partir del fin de la etapa 1, página 3 Ver Cronograma
3.4	Etapa 3: Durará 12 meses a partir de la finalización de la etapa 2	Si	789-E 789-I	Ver Detalle del Cronograma Cumplimiento, Etapa 3: Máximo 12 meses renovable a 10 años, página Ver Cronograma
3.5	Etapa 1: Entregar el diseño de seguridad de las tarjetas a las cuatro (4) semanas después de la firma de contrato. (ver numeral 1.27.3).	Si	789-B 789-G	Ver Detalle del Cronograma Cumplimiento, Etapa 1: Implantación y Puesta en Marcha del Proyecto. Punto 1, se cumple con actividad del cronograma, actividad 16 Finalización del diseño y formato del documento. Entrega en 4 semanas a la JCE, página 2 Ver Cronograma

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

3.6	Etapa 1: 2,000 tarjetas de policarbonato genéricas con chip para pruebas a las dieciséis (16) semanas.	Si	789-B 789-G	Ver Detalle del Cronograma Cumplimiento, Etapa 1: Implantación y Puesta en Marcha del Proyecto. Punto 2: 2. Suministrar dos impresoras de policarbonato a las dieciséis (16) semanas, así como 2,000 tarjetas genéricas de policarbonato con chip para pruebas. Ver Cronograma
3.7	Etapa 1: Instalar la PKI y la CA, así como realizar la ceremonia de llaves a las dieciséis (16) semanas.	Si	789-B 789-G a 789-I	Ver Detalle del Cronograma Cumplimiento, Etapa 1: Implantación y Puesta en Marcha del Proyecto.3. Instalar la PKI y la CA, así como realizar la ceremonia de llaves a las dieciséis (16) semanas. Instalar la PKI de Tarjeta Física y Digital Actividad 34: Ceremonia de entrega de llaves realizada Cumple: Entrega en 14 semanas. Instalar la PKI CA: Actividad 226: Ceremonia de Llaves Cumple: 15 semanas Ver Cronograma
3.8	Etapa 1: Entrega de 300,000 tarjetas de policarbonato a las veintidós (22) semanas después de la firma de contrato.	Si	789-B 789-G a 789-I	Ver Detalle del Cronograma Cumplimiento, Etapa 1: Implantación y Puesta en Marcha del Proyecto.Punto 7. Entrega de 300,000 tarjetas de policarbonato a las veintidós (22) semanas después de la firma de contrato. Esta entrega será acompañada con el reporte de laboratorio certificado e independiente, de los test de durabilidad de la tarjeta, así como el chip. Actividad 249: Envío, importación y entrega de documentos genéricos (2000 unidades) Cumple: Semana 13 Ver Cronograma
3.9	Etapa 1: Suministrar dos impresoras de policarbonato a las dieciséis (16) semanas.	Si	789-B 789-G	Ver Detalle del Cronograma Cumplimiento, Etapa 1: Implantación y Puesta en Marcha del Proyecto.Punto 2. Suministrar dos impresoras de policarbonato a las dieciséis (16) semanas, así como 2,000 tarjetas genéricas de policarbonato con chip para pruebas. Actividad 34: Entrega de 2 impresoras de personalización Cumple: Entrega en 16 semanas a la JCE. Ver Cronograma

CONSORCIO EMDOC
EMDOCC
CONSORCIO
Santo Domingo, R.D.

3.10	Etapa 1: Instalación de la CA y la PKI, así como realizar la ceremonia de entrega de llaves a las dieciséis (16) semanas.	Si	789-B 789-G a 789-I	Ver Detalle del Cronograma Cumplimiento, Etapa 1: Implantación y Puesta en Marcha del Proyecto.Punto 3. Instalar la PKI y la CA, así como realizar la ceremonia de llaves a las dieciséis (16) semanas. Instalar la PKI de Tarjeta Física y Digital Actividad 34: Ceremonia de entrega de llaves realizada Cumple: Entrega en 14 semanas. Instalar la PKI CA: Actividad 226: Ceremonia de Llaves Cumple: 15 semanas Ver Cronograma
3.11	Etapa 1: Realizar las pruebas piloto de la solución digital de la tarjeta CD (Mobile ID) antes de veintiséis (26) semanas, incluyendo el desarrollo de una app para la JCE.	Si	789-B 789-G a 789-I	Ver Detalle del Cronograma Cumplimiento, las actividades listadas se cumplen hasta la semana 20, punto 6. Realizar pruebas piloto de solución digital de la tarjeta CD (Mobile ID) antes veintiséis (26) semanas, incluyen el desarrollo de una app para la JCE (siempre que la JCE cumpla con sus dependencias a tiempo). página 2 Ver Cronograma
3.12	Etapa 1: Ayudar a los técnicos de la JCE a ladaptar la SDK de la impresora al sistema de la JCE. Realizar pruebas unitarias de integraciób, de pre-producción de las impresoras, las tarjelas.	Si	789-B 789-G a 789-I	Ver Detalle del Cronograma Cumplimiento, las actividades listadas se cumplen en punto No. 4. Ayudar a los técnicos de la JCE a adaptar el SDK de la impresora al sistema de la JCE. Actividad 36: Apoyo al técnico de JCE para adaptar las impresoras del SDK al sistema. Cumple: Semana 6 a 9
3.13	Etapa 1: Capacitación al personal de la JCE de la operación y mantenimiento del equipo de impresión, PKI y solución digital.	Si	789-C a 789-I	Ver Detalle del Cronograma Cumplimiento, las actividades listadas se cumplen en punto No. 8. Capacitación del personal de la JCE de la operación y mantenimiento del equipo de impresión, PKI y solución digital. JCE. Tareas 40, 57,74,87. Formación 208,230,254,266

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

3.14	Etapa 2: Suministro de inventario de tarjetas 500,000 tarjetas de Policarbonato a las 26 semanas después de la firma de contrato. 1,200,000 tarjetas de Policarbonato a las 30 semanas después de la firma de contrato. 1,000,000 tarjetas de Policarbonato a las 34 semanas después de la firma de contrato. 1,000,000 tarjetas de Policarbonato a las 38 semanas después de la firma de contrato. 1,000,000 tarjetas de Policarbonato a las 42 semanas después de la firma de contrato. 1,000,000 tarjetas de Policarbonato a las 46 semanas después de la firma de contrato. 1,000,000 tarjetas de Policarbonato a las 50 semanas después de la firma de contrato. 1,000,000 tarjetas de Policarbonato a las 54 semanas después de la firma de contrato.	Si	289-C 789-G	Ver Detalle del Cronograma Cumplimiento, Etapa 2: Máximo 12 meses a partir del fin de la etapa 1: 1. 500,000 tarjetas de policarbonato a las 26 semanas después de la firma de contrato. Cumple: Semana 26, tarea 25 2. 1,200,000 tarjetas de policarbonato a las 30 semanas después de la firma de contrato. Cumple: Semana 30, tarea 26 3. 1,000,000 tarjetas de policarbonato a las 34 semanas después de la firma de contrato. Cumple: Semana 34, tarea 27 4. 1,000,000 tarjetas de policarbonato a las 38 semanas después de la firma de contrato. Cumple: Semana 38, tarea 28 5. 1,000,000 tarjetas de policarbonato a las 42 semanas después de la firma de contrato. Cumple: Semana 42, tarea 29 6. 1,000,000 tarjetas de policarbonato a las 46 semanas después de la firma de contrato. Cumple: Semana 46, tarea 30 7. 1,000,000 tarjetas de policarbonato a las 50
3.15	Etapa 2: Ver 1.27.4 Adquisición e instalación de los equipos de impresión y puesta en marcha en las sedes de la República Dominicana y en el exterior. Las fechas de las entregas y cantidades de dichos equipos serán acordados con el proveedor adjudicado y la JCE. Puesta en marcha del mantenimiento de las impresoras en periodo de garantía. Para ello, el proveedor deberá de disponer de mínimo de dos (2) técnicos certificados en tecnología de impresión de tarjetas de identidad, y mínimo un total de diez (10) técnicos para soporte nacional de servicio para reparación de equipos en sitio durante el periodo de garantía. Para el exterior, el proveedor durante tiempo de garantía de las impresoras, deberá reparar en Nueva York (los equipos de Estados Unidos y Canadá) y en Madrid (los equipos de Europa), la JCE enviará las impresoras defectuosas a estos lugares según aplique.	Si	789-C a 789-D 190-203 482-585	Adquisición e instalación de los equipos de impresión y puesta en marcha en las sedes de laRepública Dominicana y en el exterior. Las fechas de las entregas y cantidades de dichos equipos serán acordados con el proveedor adjudicado y la JCE. El Consorcio EMDOC entregará las siguientes impresoras de la siguiente manera: 4 • Entrega 2: 90 impresoras en Santo Domingo,tarea 46, semana 24, para distribuir en R. Dominicana. • Entrega 3: 90 impresoras en Santo Domingo, tarea 60, semana 28 para distribuir en 72 en R. Dominicana y 18 que la JCE reembarcará para N. York. • Entrega 4: 32 impresoras en Santo Domingo, tarea 89, semana 36 para reembarcar de la siguiente manera: o 11 N. York: 9 USA y 2 Canadá o 15 Madrid para distribuir en Madrid o El resto serán entregadas en R.Dominicana para distribuir según señale la JCE. Vease Sección ITEM 81. PARTE B. Especificaciones del Mantenimiento Curriculum del personal técnico certificado

JCE-CCC-LPI-2024-001				
Se debe de rellenar el apartado cumple y no cumple, con la pagina del oferente donde lo cumple, asi como comentarios adicionales si procede				
No.		**Cumple/No Cumple**	**Página del oferente**	**Comentarios**
1	**REQUERIMIENTOS TÉCNICOS (NO SUBSANABLES)**			
1.1	Las tarjetas constituyen un elemento clave y deben ser fabricadas por un integrante del cons	Si	3	ITEM I Propuesta Especificaciones Técnicas de las Tarjetas - Ver Sección 1 Documentos de la Tarjeta
1.2	Se solicitan tarjetas de policarbonato para las nuevas CI y CIE, con chip sin contacto (contactless) con funcionalidad de Documento de Viaje Electrónico, Firma Electrónica e Identificación Ciudadana. Tarjeta sin contacto de acuerdo a ISO/IEC 14443.	Si	8	ITEM I Propuesta Especificaciones Técnicas de las Tarjetas - Ver Sección 1.2 Tipos de Tarjetas
1.3	Varia el color unicamente. Dos colores (fondo preimpreso) de tarjeta Tarjeta para la Cédula de Identidad y Electoral Tarjeta para la Cédula de Identidad.	Si	8	ITEM I Propuesta Especificaciones Técnicas de las Tarjetas - Ver Sección 1.2 Tipos de Tarjetas
1.4	Las dimensiones y sus tolerancias vendrán especificadas por el formato ID-1 tal y como se especifica en las normativas ISO/IEC 7816:2019 / ISO/IEC 7810:2019.	Si	7	ITEM I Propuesta Especificaciones Técnicas de las Tarjetas - Ver Sección 1.1 Características Generales
1.5	**Materiales**			
1.5.1	Tarjeta de polímero termoplástico (policarbonato) de gran resistencia, formada por varias capas (mínimo 5) fusionadas mediante laminación en caliente resistente a la división.	Si	7	ITEM I Propuesta Especificaciones Técnicas de las Tarjetas - Ver Sección 1.1 Características Generales
1.5.2	Tintas de formulación especificas para el sistema de impresión offset.	Si	7	ITEM I Propuesta Especificaciones Técnicas de las Tarjetas - Ver Sección 1.1 Características Generales
1.5.3	Tintas de seguridad con pigmento sólido.	Si	7	ITEM I Propuesta Especificaciones Técnicas de las Tarjetas - Ver Sección 1.1 Características Generales
1.5.4	Tintas ópticamente variables.	Si	7	ITEM I Propuesta Especificaciones Técnicas de las Tarjetas - Ver Sección 1.1 Características Generales
1.5.5	Elemento holográfico borde a borde o 2 Elementos holográficos o OVD en cada cédula, uno	Si	7	ITEM I Propuesta Especificaciones Técnicas de las Tarjetas - Ver Sección 1.1 Características Generales
1.5.6	Todas las tintas deberán cumplir la normativa de durabilidad (ISO 18745) y deberán tener un	Si	7	ITEM I Propuesta Especificaciones Técnicas de las Tarjetas - Ver Sección 1.1 Características Generales
1.6	**Caracteristicas de seguridad principales**			
1.6.1	Los diseños de seguridad del documento serán entregados por el adjudicatario a la JCE en f	Si	20-21	ITEM I Propuesta Especificaciones Técnicas de las Tarjetas - Ver Sección 1.4 Características Clave de Seguridad
1.6.2	Nivel 1: Impresión en iris: lineas que durante su recorrido cambian paulatinamente de color s	Si	22	ITEM I Propuesta Especificaciones Técnicas de las Tarjetas - Ver Sección 1.5.1 Funciones de Seguridad Nivel 1,2 y 3
1.6.3	Nivel 1: Guilloches: movimientos lineales ornamentales que se conforman de múltiples curvas entrecruzadas, elaboradas simultáneamente, formando complejos diseños creados mediante software de seguridad.	Si	22	ITEM I Propuesta Especificaciones Técnicas de las Tarjetas - Ver Sección 1.5.1 Funciones de Seguridad Nivel 1,2 y 3
1.6.4	Nivel 1: Numismáticos: conjunto de lineas que en su trayecto sufren una deformación y su c	Si	22	ITEM I Propuesta Especificaciones Técnicas de las Tarjetas - Ver Sección 1.5.1 Funciones de Seguridad Nivel 1,2 y 3
1.6.5	Nivel 1: Tinta ópticamente variable: aquella que contiene en su estructura finas particulas que dotan el efecto óptico de variabilidad cuando se cambia el ángulo de incidencia de la luz y de observación. Son visibles a la radiación IR.	Si	22	ITEM I Propuesta Especificaciones Técnicas de las Tarjetas - Ver Sección 1.5.1 Funciones de Seguridad Nivel 1,2 y 3
1.6.6	Nivel 1: Elemento difractivo ópticamente variable, situado en el interior de la tarjeta, ocupando parcialmente la zona de la fotografía del titular. Como se explica más adelante, este elemento también puede incluir medidas de nivel 2 y en algunos casos de nivel 3.	Si	22	ITEM I Propuesta Especificaciones Técnicas de las Tarjetas - Ver Sección 1.5.1 Funciones de Seguridad Nivel 1,2 y 3
1.6.7	Nivel 1: Elementos táctiles en alto o bajo relieve o con acabado mate, integrados en la superficie de la tarjeta. Personalización en relieve con el láser de la personalización del nombre y del número de tarjeta. Se espera que se contengan tanto en la tarjeta sin personalizar como que el proceso de personalización permita dotar elementos táctiles a la tarjeta.	Si	22	ITEM I Propuesta Especificaciones Técnicas de las Tarjetas - Ver Sección 1.5.1 Funciones de Seguridad Nivel 1,2 y 3
1.6.9	Nivel 2: Microtextos. Impresión positivo y negativo. Microtexto de fluorescencia.	Si	22	ITEM I Propuesta Especificaciones Técnicas de las Tarjetas - Ver Sección 1.5.1 Funciones de Seguridad Nivel 1,2 y 3
1.6.10	Nivel 2: UV Malla de fondo en microtexto.	Si	22	ITEM I Propuesta Especificaciones Técnicas de las Tarjetas - Ver Sección 1.5.1 Funciones de Seguridad Nivel 1,2 y 3

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

1.6.11	Nivel 2: Errores deliberados en el documento.	Si	22	ITEM I Propuesta Especificaciones Técnicas de las Tarjetas - Ver Sección 1.5.1 Funciones de Seguridad Nivel 1,2 y 3
1.6.12	Nivel 2: Tinta invisible que fluórese bajo luz ultravioleta. Impresión arcoiris visible (impresión arcoiris offset). Impresión arcoíris invisible (impresión arcoíris de fluorescencia UV).	Si	22	ITEM I Propuesta Especificaciones Técnicas de las Tarjetas - Ver Sección 1.5.1 Funciones de Seguridad Nivel 1,2 y 3
1.6.13	Nivel 2: Fondos de seguridad visibles e invisibles en la zona de la fotografía, para detectar p	Si	22	ITEM I Propuesta Especificaciones Técnicas de las Tarjetas - Ver Sección 1.5.1 Funciones de Seguridad Nivel 1,2 y 3
1.6.14	Nivel 2: Tipo de fuente no estándar para elementos de texto impresos.	Si	22	ITEM I Propuesta Especificaciones Técnicas de las Tarjetas - Ver Sección 1.5.1 Funciones de Seguridad Nivel 1,2 y 3
1.6.15	Nivel 3: Tarjeta Multicapa 5 capas mínimo.	Si	22	ITEM I Propuesta Especificaciones Técnicas de las Tarjetas - Ver Sección 1.5.1 Funciones de Seguridad Nivel 1,2 y 3
1.6.16	Nivel 3: Tintas invisibles en el infrarrojo (para permitir la lectura mecánica del documento. Re	Si	22	ITEM I Propuesta Especificaciones Técnicas de las Tarjetas - Ver Sección 1.5.1 Funciones de Seguridad Nivel 1,2 y 3
1.6.17	Nivel 3: Nanotextos integrados en el elemento difractivo.	Si	22	ITEM I Propuesta Especificaciones Técnicas de las Tarjetas - Ver Sección 1.5.1 Funciones de Seguridad Nivel 1,2 y 3
1.6.18	Nivel 3: Fondos de seguridad visibles e invisibles en la zona de la fotografía, para detectar posibles manipulaciones o sustituciones de esta.	Si	22	ITEM I Propuesta Especificaciones Técnicas de las Tarjetas - Ver Sección 1.5.1 Funciones de Seguridad Nivel 1,2 y 3
1.6.19	Otras características de seguridad: Elemento óptico variable difractivo: Parche difractivo transparente de diseño exclusivo para la JCE, combinadas con líneas de Nanotextos y textos de formas moduladas en líneas sinusoidales. Las imágenes deberán poseer textos ocultos visibles en determinados ángulos de observación, pudiendo ser estos, cambiantes en más de un ángulo. Es válido un holograma tipo parche (patch) o de superficie completa (full surface).	Si	22-24	ITEM I Propuesta Especificaciones Técnicas de las Tarjetas - Ver Sección 1.5.1 Funciones de Seguridad Nivel 1,2, 3 y 1.5.2 Otros Dispositivos de Seguridad
1.6.20	Otras características de seguridad: Elementos Táctiles: Deberán ser integrados en la estructura de la tarjeta, en el anverso de esta, durante el proceso de fabricación. El diseño de estos elementos deberá ser aceptado por la JCE.	Si	22-24	ITEM I Propuesta Especificaciones Técnicas de las Tarjetas - Ver Sección 1.5.1 Funciones de Seguridad Nivel 1,2, 3 y 1.5.2 Otros Dispositivos de Seguridad
1..6.21	Otras características de seguridad: Ventana Transparente: Deberá incluir una ventana transparente.	Si	22-24	ITEM I Propuesta Especificaciones Técnicas de las Tarjetas - Ver Sección 1.5.1 Funciones de Seguridad Nivel 1,2, 3 y 1.5.2 Otros Dispositivos de Seguridad
1.6.22	Otras características de seguridad: Estructura Lenticular: Deberá incluir una estructura lenticular para personalización de un CLI.	Si	22-24	ITEM I Propuesta Especificaciones Técnicas de las Tarjetas - Ver Sección 1.5.1 Funciones de Seguridad Nivel 1,2, 3 y 1.5.2 Otros Dispositivos de Seguridad
1.6.23	Otras características de seguridad: Protección del Retrato del titular: Mediante elemento ópticamente variable de tipo difractivo transparente, parcialmente coincidente con el retrato del titular.	Si	22-24	ITEM I Propuesta Especificaciones Técnicas de las Tarjetas - Ver Sección 1.5.1 Funciones de Seguridad Nivel 1,2, 3 y 1.5.2 Otros Dispositivos de Seguridad
1.6.24	Otras características de seguridad: Numeración de la Tarjeta: Se identificará individualmente cada tarjeta mediante número de serie de tarjeta pre personalizado en grabado láser	Si	22-24	ITEM I Propuesta Especificaciones Técnicas de las Tarjetas - Ver Sección 1.5.1 Funciones de Seguridad Nivel 1,2, 3 y 1.5.2 Otros Dispositivos de Seguridad
1.6.25	Durabilidad: Se garantizará la durabilidad del soporte por un período de 10 años.	Si	24	ITEM I Propuesta Especificaciones Técnicas de las Tarjetas - Ver Sección 1.5.3 Resistencia de la Tarjeta según la OACI
1.6.26	Toxicidad: No deberá presentar ningún riesgo tóxico en su uso normal.	Si	24	ITEM I Propuesta Especificaciones Técnicas de las Tarjetas - Ver Sección 1.5.3 Resistencia de la Tarjeta según la OACI
1.6.27	Deformación: De tal naturaleza la deformación causada por el uso normal, puedan enderezarse con el equipo de lectura sin afectar el uso de la tarjeta ni su funcionamiento. Ejemplo es la lectura del MRZ no debe deformar la tarjeta.	Si	24	ITEM I Propuesta Especificaciones Técnicas de las Tarjetas - Ver Sección 1.5.3 Resistencia de la Tarjeta según la OACI
1.6.28	Resistencia a productos químicos: Será resistente a los efectos químicos inherentes al manejo y uso normales, salvo cuando se le haya dotado de sensibilidad química por razones de seguridad.	Si	24	ITEM I Propuesta Especificaciones Técnicas de las Tarjetas - Ver Sección 1.5.3 Resistencia de la Tarjeta según la OACI
1.6.29	Estabilidad térmica: Se mantendrá legible mecánicamente a temperaturas que oscilen entre -10 °C y +50 °C. La tarjeta no perderá su funcionalidad en caso de quedar expuesto a temperaturas que oscilen entre -35 °C y + 80 °C.	Si	24	ITEM I Propuesta Especificaciones Técnicas de las Tarjetas - Ver Sección 1.5.3 Resistencia de la Tarjeta según la OACI

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

1.6.30	Humedad: La tarjeta será legible mecánicamente a una humedad relativa a ambiente del 5 % al 95 % y una temperatura máxima de bulbo húmedo de 25 °C. La tarjeta no perderá su fiabilidad en caso de quedar almacenada o expuesta a una humedad relativa ambiente del 0 % al 100 % (sin condensación).	Si	24	ITEM I Propuesta Especificaciones Técnicas de las Tarjetas - Ver Sección 1.5.3 Resistencia de la Tarjeta según la OACI
1.7	**Características electrónicas y sistema operativo**			
1.7.1	Las funcionalidades electrónicas serán operativas una vez se haga una activación mediante	Si	33	ITEM I Propuesta Especificaciones Técnicas de las Tarjetas - Ver Sección 1.5.5 Características Electrónicas y Sistema Operativo
1.7.3	No se prevé que el documento pueda cambiar o ampliar su funcionalidad una vez se haya entregado al ciudadano, con excepción de los certificados de firma digital que podrán tener un vencimiento diferente al documento físico en cuyo caso se deberá prever la administración de todo el ciclo de vida de los mismos (generación, actualización y revocación) en la electrónica de los documentos	Si	90-92	ITEM III Propuesta Especificaciones Técnicas de la PKI - Ver Sección 1.7 Características de la PKI Propuesta
1.7.4	Vencimiento de Certificados de CA raiz de 10-20 años	Si	90-92	ITEM III Propuesta Especificaciones Técnicas de la PKI - Ver Sección 1.7 Características de la PKI Propuesta
1.7.5	Vencimiento de Certificados Intermedios 5-10 años	Si	90-92	ITEM III Propuesta Especificaciones Técnicas de la PKI - Ver Sección 1.7 Características de la PKI Propuesta
1.7.6	Vencimiento de Certificados de Usuario Final y Servidor 1-3 años	Si	90-92	ITEM III Propuesta Especificaciones Técnicas de la PKI - Ver Sección 1.7 Características de la PKI Propuesta
1.7.7	Se debe proveer la funcionalidad de revocación de certificados y sello de tiempos	Si	90-92	ITEM III Propuesta Especificaciones Técnicas de la PKI - Ver Sección 1.7 Características de la PKI Propuesta
1.7.8	Se requiere portal web de gestión de ciclo de vida de certificados (emisión y revocación) para la JCE que debe acceder con su certifcado de autenticación. Se podrá realizar consultas o reportes de los certificados.	Si	90-92	ITEM III Propuesta Especificaciones Técnicas de la PKI - Ver Sección 1.7 Características de la PKI Propuesta
1.7.9	**Características del chip sin contacto**			
1.7.3.1	CPU de 16/32 bits.	Si	33	ITEM I Propuesta Especificaciones Técnicas de las Tarjetas - Ver Sección 1.5.5.1 Características del chip sin contacto
1.7.3.2	Certificación CC EAL5+ o superior (o equivalente).	Si	33	ITEM I Propuesta Especificaciones Técnicas de las Tarjetas - Ver Sección 1.5.5.1 Características del chip sin contacto
1.7.3.3	Criptoprocesador hardware para operaciones criptográficas.	Si	33	ITEM I Propuesta Especificaciones Técnicas de las Tarjetas - Ver Sección 1.5.5.1 Características del chip sin contacto
1.7.3.4	Clave simétrica (Triple DES con clave de hasta 168 bits, AES hasta 256 bits).	Si	33	ITEM I Propuesta Especificaciones Técnicas de las Tarjetas - Ver Sección 1.5.5.1 Características del chip sin contacto
1.7.3.5	Clave pública (RSA con longitud de clave de hasta 4096 y ECC con clave de hasta 512 bits	Si	33	ITEM I Propuesta Especificaciones Técnicas de las Tarjetas - Ver Sección 1.5.5.1 Características del chip sin contacto
1.7.3.6	Hash SHA1 y SHA2.	Si	33	ITEM I Propuesta Especificaciones Técnicas de las Tarjetas - Ver Sección 1.5.5.1 Características del chip sin contacto
1.7.3.7	Generador de números aleatorios de acuerdo a AIS31 Protección contra descargas ESD.	Si	33	ITEM I Propuesta Especificaciones Técnicas de las Tarjetas - Ver Sección 1.5.5.1 Características del chip sin contacto
1.7.3.8	Reloj interno asíncrono Número de serie único.	Si	33	ITEM I Propuesta Especificaciones Técnicas de las Tarjetas - Ver Sección 1.5.5.1 Características del chip sin contacto
1.7.3.9	Firewalls de seguridad entre particiones de memoria.	Si	33	ITEM I Propuesta Especificaciones Técnicas de las Tarjetas - Ver Sección 1.5.5.1 Características del chip sin contacto
1.7.3.10	Memoria no volátil necesaria para la incorporación de las aplicaciones requeridas y los datos especificados en el presente punto 1.2.4. Características electrónicas y del sistema operativo.	Si	33	ITEM I Propuesta Especificaciones Técnicas de las Tarjetas - Ver Sección 1.5.5.1 Características del chip sin contacto
1.7.3.11	Retención de datos en memoria no volátil de al menos 10 años.	Si	33	ITEM I Propuesta Especificaciones Técnicas de las Tarjetas - Ver Sección 1.5.5.1 Características del chip sin contacto
1.7.3.12	Al menos 500.000 ciclos de lectura / escritura garantizados Interfaz de RF ISO/IEC 14443 A/B de hasta 848kbits/s, pudiendo ofrecer modos de transmisión RF mejorados.+	Si	33	ITEM I Propuesta Especificaciones Técnicas de las Tarjetas - Ver Sección 1.5.5.1 Características del chip sin contacto
1.7.4	**Características del Sistema Operativo**			
1.7.4.1	Protocolo de transmisión de acuerdo con ISO/IEC 14443 A/B Interfaz de comandos de acue	Si	34	ITEM I Propuesta Especificaciones Técnicas de las Tarjetas - Ver Sección 1.5.5.2 Características del sistema operativo

CONSORCIO EMDOC
EMDOC CONSORCIO
Santo Domingo, RD

1.7.4.2	UID / PUPI aleatorio.	Si	34	ITEM I Propuesta Especificaciones Técnicas de las Tarjetas - Ver Sección 1.5.5.2 Características del sistema operativo
1.7.4.3	En caso de que el Sistema Operativo sea basado en JavaCard, se deberá bloquear la posibilidad del agregado de nuevas aplicaciones una vez incorporadas las aplicaciones requeridas.	Si	34	ITEM I Propuesta Especificaciones Técnicas de las Tarjetas - Ver Sección 1.5.5.2 Características del sistema operativo
1.7.5.	**Funcionalidad de documento de viaje electrónico:**			
1.7.5.1	Deberá poder soportar: SAC (Supplemental Access Control).EAC (Extended Access Control). AA (Active Authentication)	Si	34	ITEM I Propuesta Especificaciones Técnicas de las Tarjetas - Ver Sección 1.5.5.2 Características del sistema operativo
1.7.6	**Funcionalidad de Firma Electrónica:**			
1.7.6.1	Acceso protegido mediante PIN / PUK.	Si	34	ITEM I Propuesta Especificaciones Técnicas de las Tarjetas - Ver Sección 1.5.5.2 Características del sistema operativo
1.7.6.2	Algoritmos de firma RSA y ECDSA.	Si	34	ITEM I Propuesta Especificaciones Técnicas de las Tarjetas - Ver Sección 1.5.5.2 Características del sistema operativo
1.7.6.3	Soporte para claves RSA en formato CRT y en formato normal (exponente privado, exponente público y módulo).	Si	34	ITEM I Propuesta Especificaciones Técnicas de las Tarjetas - Ver Sección 1.5.5.2 Características del sistema operativo
1.7.6.4	Claves RSA con soporte para componentes p y q de longitud variable.	Si	34	ITEM I Propuesta Especificaciones Técnicas de las Tarjetas - Ver Sección 1.5.5.2 Características del sistema operativo
1.7.6.5	Capacidad de almacenar, generar y usar claves RSA de, como mínimo, 4096 bits de longitud (autoridad raíz y Subordinada). Para el caso de los certificados de ciudadanos será de 2048 bits. Las claves que componen la "PKI de Firma Digital" y la "PKI de Firma de Documentos" deben estár basadas en los estándares X.509v3 y el RFC 5280. Se debe tener la capacidad de soportar curvas elípticas NIST P-256, BrainpoolP256r1, entre otras, conforme con los estándares: oTR-03111 Elliptic Curve Cryptography (ECC) based on ISO 15946. Technical Guideline TR-03111, Version 2.0 oISO15946-1 ISO/IEC. 15946-1. Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 1: General. 2002. oISO15946-2 ISO/IEC. 15946-2. Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 2: Digital signatures. 2002. oISO15946-3 ISO/IEC. 15946-3: Information technology — Security techniques — Cryptographic techniques based on elliptic curves — Part 3: Key establishment. 2002. oEl eID debe ser capaz de almacenar certificados x.509 que permitan a los ciudadanos gozar de los servicios de criptografía.	Si	34	ITEM I Propuesta Especificaciones Técnicas de las Tarjetas - Ver Sección 1.5.5.2 Características del sistema operativo
1.7.6.6	Soporte de diversas curvas ECDSA, incluyendo las más habituales (NIST P-256, Brainpool, etc.	Si	34	ITEM I Propuesta Especificaciones Técnicas de las Tarjetas - Ver Sección 1.5.5.2 Características del sistema operativo
1.7.6.7	Operaciones de firma digital.	Si	34	ITEM I Propuesta Especificaciones Técnicas de las Tarjetas - Ver Sección 1.5.5.2 Características del sistema operativo
1.7.6.8	Intercambio de claves de sesión o simétricas entre dos entidades basado en RSA/ECDSA/ECDH.	Si	34	ITEM I Propuesta Especificaciones Técnicas de las Tarjetas - Ver Sección 1.5.5.2 Características del sistema operativo
1.7.6.9	Claves almacenadas en ficheros/elementos independientes.	Si	34	ITEM I Propuesta Especificaciones Técnicas de las Tarjetas - Ver Sección 1.5.5.2 Características del sistema operativo
1.7.6.10	Condiciones de acceso independientes para cada clave/elemento.	Si	34	ITEM I Propuesta Especificaciones Técnicas de las Tarjetas - Ver Sección 1.5.5.2 Características del sistema operativo
1.7.6.11	Estructura interna de ficheros según el estándar ISO/IEC 7816-15 (PKCS#15). Para mayor claridad, la "Aplicación de firma electrónica" debe de estar certificada conforma CC EAL5+, ser compatible con el conjunto y comandos ISO-7816.	Si	34	ITEM I Propuesta Especificaciones Técnicas de las Tarjetas - Ver Sección 1.5.5.2 Características del sistema operativo
1.7.6.12	Deberá disponer de capacidad de memoria suficiente para almacenar hasta 4 certificados, con sus correspondientes claves, incluyendo el caso de claves RSA 4096.	Si	34	ITEM I Propuesta Especificaciones Técnicas de las Tarjetas - Ver Sección 1.5.5.2 Características del sistema operativo
1.7.6.13	Securización de los mensajes transmitidos entre la tarjeta y el terminal mediante canal seguro de acuerdo a CEN14890 o equivalente.	Si	34	ITEM I Propuesta Especificaciones Técnicas de las Tarjetas - Ver Sección 1.5.5.2 Características del sistema operativo
1.7.6.14	Confidencialidad de los datos transmitidos mediante triple DES / AES.	Si	34	ITEM I Propuesta Especificaciones Técnicas de las Tarjetas - Ver Sección 1.5.5.2 Características del sistema operativo
1.7.6.15	Autenticación de la información intercambiada entre las dos partes; incorporación de checksum criptográfico de tipo MAC según ANSI X9.19 y DES.	Si	34	ITEM I Propuesta Especificaciones Técnicas de las Tarjetas - Ver Sección 1.5.5.2 Características del sistema operativo

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

1.7.6.16	Protocolo de establecimiento de las claves de sesión basado en el esquema propuesto en ISO/IEC 9798-3 Authentication SASL Mechanism.	Si	35	ITEM I Propuesta Especificaciones Técnicas de las Tarjetas - Ver Sección 1.5.5.2 Caracteristicas del sistema operativo
1.7.6.17	Claves de sesión derivadas a partir de información generada por las partes involucradas en el establecimiento del canal seguro; el cálculo de las claves se realiza según ANSI X9.63.	Si	35	ITEM I Propuesta Especificaciones Técnicas de las Tarjetas - Ver Sección 1.5.5.2 Características del sistema operativo
1.7.6.18	Drivers de la tarjeta (PKCS#11, CSP, Card Module, etc).	Si	35	ITEM I Propuesta Especificaciones Técnicas de las Tarjetas - Ver Sección 1.5.5.2 Características del sistema operativo
1.7.6.19	Software de gestión que permita gestionar las operaciones más habituales con la tarjeta; por ejemplo, cambio de PIN, desbloqueo de PIN, borrado de certificados, etc. Deberá garantizar el funcionamiento del documento en distintos sistemas operativos (Windows, Linux, MacOS). Deberá garantizar el funcionamiento del documento en distintos navegadores. Se hace referencia a las operaciones de emision, aprovisionamiento, despliegue, inventario, aseguramiento, monitoreo, renovacion, y demas acciones habituales del uso de certificados digitales.	Si	35	ITEM I Propuesta Especificaciones Técnicas de las Tarjetas - Ver Sección 1.5.5.2 Características del sistema operativo
1.7.6.20	Se deberán aportar librerías o SDKs que faciliten el desarrollo de aplicaciones para dispositivos móviles, con sistemas operativos Android e iOS.	Si	35	ITEM I Propuesta Especificaciones Técnicas de las Tarjetas - Ver Sección 1.5.5.2 Características del sistema operativo
1.7.6.21	El software suministrado deberá ser actualizado, adecuándolo a nuevos SO, Navegadores, corrección de bugs, etc., durante el tiempo de vida del proyecto.	Si	35	ITEM I Propuesta Especificaciones Técnicas de las Tarjetas - Ver Sección 1.5.5.2 Características del sistema operativo
1.7.7	**Funcionalidad de Identificación Ciudadana:**			
1.7.7.1	Se almacenarán los datos de filiación del ciudadano de manera estructurada.	Si	35	ITEM I Propuesta Especificaciones Técnicas de las Tarjetas - Ver Sección 1.5.5.2 Características del sistema operativo
1.7.7.1	El acceso a los mismos se realizará por medios seguros.	Si	35	ITEM I Propuesta Especificaciones Técnicas de las Tarjetas - Ver Sección 1.5.5.2 Características del sistema operativo
1.7.7.1	Preferiblemente, de acuerdo con la Guía Técnica TR-03110 del BSI o similar.	Si	35	ITEM I Propuesta Especificaciones Técnicas de las Tarjetas - Ver Sección 1.5.5.2 Características del sistema operativo
1.7.8	**Muestras:**			
1.7.8.1	El oferente deberá, en el momento de entregar las ofertas, suministrar diez (10) tarjetas genéricas de policarbonato, con las mismas especificaciones técnicas que se solicitan para esta licitación y con el detalle y la explicación de las medidas de seguridad que el oferente está ofreciendo, explicando en un documento, cuáles son los requisitos técnicos cumplidos y las medidas de seguridad ofertadas, excepto el diseño. En las tarjetas de muestra se podrá mostrar sólo el applet ICAO. El applet eID es opcional. Los chips para estas tarjetas podrán no ser exactamente los mismos que usarán más adelante en los 8 millones de tarjetas reales.Las muestras pueden ser sin el elemento holográfico. Este es un requisito obligatorio (mandatorio) no subsanable.	Si	36-41 1-164	ITEM I Propuesta Especificaciones Técnicas de las Tarjetas - Ver Sección 1.6 Tarjeta de Muestra Ver Pruebas Independientes de acuerdo a la Norma ISO 18745 Muestras 10, sobre A, páginas 1-164
2	**Maquinas de Impresión**			
2.1.	**Especificiones de Máquinas de impresión**			
2.1.1	Máquina de impresión modular. (se le pueden añadir o quitar módulos, por ejemplo, para inc	Si	58	ITEM II Máquinas de Impresión - Ver Sección 1.1 Máquina de Impresión
2.1.2	La tecnología de personalización deberá ser de grabado láser, siendo para la fotografía láser con escala de grises.	Si	58	ITEM II Máquinas de Impresión - Ver Sección 1.1 Características Generales de la Máquina de Impresión
2.1.2	El sistema de personalización propuesto será un sistema de escritorio.	Si	58	ITEM II Máquinas de Impresión - Ver Sección 1.1 Características Generales de la Máquina de Impresión
2.1.3	Tiene que ser un sistema de producción industrial sólido, para funcionamiento de la máquina en producción de 3 turnos (24 horas) si así se requiere.	Si	59	ITEM II Máquinas de Impresión - Ver Sección 1.1 Características Generales de la Máquina de Impresión
2.1.4	La máquina debe estar equipada con una conexión de alimentación monofásica de 110/220 V para su funcionamiento.Específicamente Europa y Chile 220 V, resto 110 V.	Si	59	ITEM II Máquinas de Impresión - Ver Sección 1.1 Características Generales de la Máquina de Impresión
2.1.5	Cada impresora de personalización debe estar equipada con una fuente de alimentación ininterrumpida para cubrir los PC integrados y la producción durante al menos dos minutos.	Si	59	ITEM II Máquinas de Impresión - Ver Sección 1.1 Características Técnicas
2.1.6	El peso de cada máquina debe ser de 80 kg máximo. Su volumen máximo no debe exceder de 0,70 m3.	Si	60	ITEM II Máquinas de Impresión - Ver Sección 1.1 Dimensiones
2.1.7	El sistema debe estar equipado con una pantalla para la visualización de los trabajos.	Si	60	ITEM II Máquinas de Impresión - Ver Sección 1.1 Interfaz Gráfica de Usuario

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

2.1.8	Debe estar disponible un módulo de codificación de chip. Debe permitir la codificación de tarjetas inteligentes basadas en contacto y sin contacto según ISO 14443 tipo A y B.	Si	61	ITEM II Máquinas de Impresión - Ver Sección 1.1 Conformidad
2.1.9	El sistema debe poder grabar imágenes, firmas, textos y códigos de barras (códigos de barras 1D y 2D), así como microtexto, imágenes fantasma y logotipos en tamaños variables.	Si	63	ITEM II Máquinas de Impresión - Ver Sección 1.1.5 Sistema láser
2.1.10	El sistema debe admitir el marcado láser táctil, así como la personalización de la función de la tarjeta CLI.	Si	63	ITEM II Máquinas de Impresión - Ver Sección 1.1.5 Sistema láser
2.1.11	Para garantizar la calidad, se debe integrar un sistema de control óptico de la tarjeta para una inspección completa de la tarjeta en el anverso y el reverso de forma independiente. Además, el sistema de control óptico debe realizar un proceso de inspección antes del grabado láser para alinear el diseño del grabado con el tipo de tarjeta especial. La función de detección de CLI también debe estar disponible y debe funcionar independientemente de los demás procesos de inspección de tarjetas. Se requiere una alineación de grabado láser individual del proceso de calidad CLI.	Si	63	ITEM II Máquinas de Impresión - Ver Sección 1.1.3 Sistema de Control de Tarjetas para Ajuste del Láser y 1.1.6 Sistema de Control de Tarjetas
2.1.12	Es necesario que los componentes de inspección sean ajustables para procesar diferentes diseños de tarjetas mediante el uso de una unidad de iluminación LED múltiple con diferentes longitudes de onda. El término "LED múltiple" en el requisito mencionado se refiere a los componentes del sistema de iluminación.	Si	62 65	ITEM II Máquinas de Impresión - Ver Sección 1.1.3 Sistema de Control de Tarjetas para Ajuste del Láser y 1.1.6 Sistema de Control de Tarjetas
2.1.13	La máquina debe tener su propio PC integrado con su propio sistema operativo y software de la máquina.	Si	71	ITEM II Máquinas de Impresión - Ver Sección 1.3.2 Máquina de Impresión PC interno
2.1.14	El sistema operativo de la PC debe ser WINDOWS. Las impresoras pueden ser WINDOWS o LINUX.	Si	71	ITEM II Máquinas de Impresión - Ver Sección 1.3.2 Máquina de Impresión PC interno
2.1.15	Debido a una integración de red obligatoria, los sistemas propuestos necesitan tener una interfaz TCP/IP para funcionar con ellos como una estación de trabajo completa con su propia dirección IP, que puede definirse y ajustarse.	Si	71	ITEM II Máquinas de Impresión - Ver Sección 1.3.3 Integración en la red
2.1.16	La solución propuesta debe ser capaz de identificar los registros inconsistentes antes de proceder con la impresión de la tarjeta. Si el registro enviado por la interfaz de integración está incompleto, por la ausencia de alguno de los datos requeridos, el registro debe ser rechazado,	Si	68-69	ITEM II Máquinas de Impresión - Ver Sección 1.3.1 Preparación de datos, incoherencia, firma de documentos, función de gestión de claves
2.1.17	La solución propuesta solo debe almacenar los datos de forma temporal. El almacenamiento temporal se refiere a que en ningún momento la solución almacenará registros por más de un día. Es decir, una vez impresa y entregada la tarjeta, el registro debe eliminarse de forma criptográfica de todos los servidores de la solución donde este almacenada. El procedimiento de eliminación de los registros ya procesados debe ser aprobado por la JCE.	Si	69-70	ITEM II Máquinas de Impresión - Ver Sección 1.3.1 Apoyo a la presentación de informes
2.1.18	El tipo de láser debe ser láser de fibra mínimo de 20W.	Si	63	ITEM II Máquinas de Impresión - Ver Sección 1.1.5 Sistema láser
2.1.19	Deberá ser posible definir los ejes de referencia sobre el insumo a fin de configurar el. posicionamiento para el marcado láser. Esta definición deberá ser tanto automática como plausible de definirla por una interfase accesible por los técnicos de la JCE.	Si	73-74	ITEM II Máquinas de Impresión - Ver Sección 1.4.2 Edición del diseño de la tarjeta por personal autorizado
2.1.1.20	ELIMINADO	Seleccionar		
2.1.12	La eficiencia productiva de la solución tecnológica ofrecida deberá ser superior al NOVENTA POR CIENTO (90%), calculada según cantidad de tarjetas efectivas producidas por hora / capacidad de máquina por hora informada por el fabricante.	Si	60	ITEM II Máquinas de Impresión - Ver Sección 1.1 Eficacia de la Producción
2.1.22	La calidad de las impresoras debe mantenerse a lo largo de los diez años de la contratación. Tendrán garantía mínima por dos (2) años. Cada oferente, debe indicar en su propuesta, la vida útil de las piezas de cada impresora que produce el láser y queda comprometido a que su solución de impresión mantendrá la calidad de las impresoras durante todo el tiempo que lo exige el contrato, obligándose a reemplazar lo necesario y las veces que sea conveniente para cumplir con esta exigencia de calidad de las impresoras.	Si	60	ITEM II Máquinas de Impresión - Ver Sección 1.1 Calidad de las Impresoras y Garantía

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

2.1.23	Los equipos deberán disponer de **un control de calidad** y registrar los eventos identificados, garantizando: - Evaluación de funcionamiento del chip antes de su personalización. - Correcto grabado del chip después de su personalización. - Control de información grabada durante la personalización de la tarjeta de policarbonato. - Control de espesor, orientación de la tarjeta y referencia. - Control de MRZ (ZLM). - Control de texto. - Control de los datos del chip. - Control de los datos gráficos.	Si	64	ITEM II Máquinas de Impresión - Ver Sección 1.1.6 Sistema de Control de Tarjetas
2.1.24	El proveedor deberá incluir 230 lectores de chip sin contacto, y poner como opcional, la compra de lectores de forma individual. La caracteristicas del lector de tarjetas debe ser Lector para NFC Compatible con ISO 14443 Tipo A, Tipo B y Tarjetas Mifare 1k&4k, ICAO 9303 con interoperabilidad OACI DOC 9303, ISO18013, PA, AA, BAC, EAC , SAC.	Si	187	COMPONENTES PARA LAS ESPECIFICACIONES DE KIT DE PERIFÉRICOS V.7 LECTOR RFID
2.1.25	El fabricante deberá describir el flujo de trabajo y los diferentes criterios que podrían ser utlizados para el control de calidad adicional. Las impresoras deben contener un módulo de administración de diagnósticos de impresión para el control de cantidades de tarjetas impresas por cada hora de uso. Los controles de calidad son dispuestos por la solución de personalización como parte de la implementación del controlador del equipo como sistema. Esto asegura que se mantenga un alto nivel de control de calidad en todo el proceso de impresión, garantizando que las impresoras administren de manera eficiente los diagnósticos y el control de cantidades de tarjetas impresas por cada hora de uso.	Si	55-67	ITEM II Máquinas de Impresión - Ver Sección 1.2 Sistema de control de máquina de impresión Mühlbauer MCES Ver 1.2.3. Herramienta de registro
2.1.26	Control ATS (Answer To Select) a la entrada, para verificación del correcto funcionamiento del chip de la tarjeta.	Si	62	ITEM II Máquinas de Impresión - Ver Sección 1.1.4Respuesta a Seleccionar (ATS) por sistema de lectura del Módulo de Garantía de Calidad
2.1.27	Los equipos deberán contar con los accesorios, equipos auxiliares y cualquier otro implemento necesario para su operación según las prestaciones especificadas en el presente pliego.	Si	79-1 a 79-3	Entregables Máquinas de Impresión
2.1.28	Deben permitir el rechazo de credenciales defectuosas por inspección y control de chip.	Si	64-65	ITEM II Máquinas de Impresión - Ver Sección 1.1.6 Sistema de Control de Tarjetas y 1.1.7 Módulo de Salida
2.2.	**Personalización**			
2.2.1	La tecnología de personalización deberá ser de grabado láser, siendo para la fotografía láser en escala de grises mínimo 600 DPI.	Si	63	ITEM II Máquinas de Impresión - Ver Sección 1.1.5 Sistema láser
2.2.2	Alimentador Automático min 100 Tarjetas.	Si	61	ITEM II Máquinas de Impresión - Ver Sección 1.1.1 Módulo de alimentación de tarjetas (entrada)
2.2.3	Bandeja salida mínimo 100 tarjetas con opción de algunas con capacidad menores.	Si	65	ITEM II Máquinas de Impresión - Ver Sección 1.1.7 Módulo de Salida
2.2.4	Velocidad MÍNIMO 50 por hora incluyendo laser a doble cara, codificación, verificación QA. Se debe presentar ficha tecnica del fabricante en su web o en su portfolio.	Si	59	ITEM II Máquinas de Impresión - Ver Sección 1.1 Rendimiento
2.2.5	Personalización de los datos (según punto II.2.1 del pliego: Fotos de Cedula Tipo).	Si	75	ITEM II Máquinas de Impresión - Ver Sección 1.6Personalización según el formato y el diseño solicitados
2.2.6	Conjunto mínimo de datos personales y del documento de acuerdo con la normativa OACI (Doc. 9303).	Si	59	ITEM II Máquinas de Impresión - Ver Sección 1.1 Conformidad
2.2.7	Líneas de lectura mecánica en la zona inferior del reverso de la tarjeta (zona de lectura mecánica o ZLM).	Si	59	ITEM II Máquinas de Impresión - Ver Sección 1.1 Conformidad
2.2.8	Imagen facial en escala de grises.	Si	63	ITEM II Máquinas de Impresión - Ver Sección 1.1.5 Sistema láser
2.2.9	Imagen fantasma o secundaria en escala de grises, en posición a definir.	Si	63	ITEM II Máquinas de Impresión - Ver Sección 1.1.5 Sistema láser
2.2.10	El sistema deberá disponer de un acceso de nivel de operador.	Si	72	ITEM II Máquinas de Impresión - Ver Sección 1.4 Interfaz de usuario

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

2.2.11	Cada entrada del operador deberá quedar reportada, con el fin de identificar cada usuario que accede a la máquina.	Si	72	ITEM II Máquinas de Impresión - Ver Sección 1.4 Interfaz de usuario
2.2.12	El sistema de personalización debe diseñarse para un manejo de documentos fácil y amigable para el operador con una separación de entrada de tarjeta sin fricción y solo la persona autorizada puede acceder a la entrada.	Si	61	ITEM II Máquinas de Impresión - Ver Sección 1.1.1 Módulo de alimentación de tarjetas (entrada)
2.2.13	El proceso de personalización de las tarjetas deberá ser tipo modular, de tal forma que la tarjeta sea trasladada automáticamente de una etapa a otra y hasta el final de su personalización (en línea) sin intervención manual del operador. La impresora deberá imprimir ambas caras de la tarjeta en un sólo proceso completo de impresión, sin volver a pasarla por el proceso.	Si	58-59	ITEM II Máquinas de Impresión - Ver Sección 1.1 Máquina de Impresión
2.2.14	Dada la obligatoriedad de integración a una red, los sistemas propuestos deberán disponer de interfaz TCP / IP para trabajar con ellos como una estación de trabajo completa con su propia dirección IP, la cual podrá ser definida y ajustada oportunamente.	Si	71	ITEM II Máquinas de Impresión - Ver Sección 1.3.3 Integración en la red
2.2.15	El sistema de personalización (software y maquinaria) debe ser capaz de imprimir diferente información acorde al menos el lay out según punto II.2.1 del pliego; deberá personalizar, según sea necesario, personas mayores de edad, menores de edad, naturalizadas, extranjeras, etc. Debe ser posible la edición del lay out accesible por la JCE.	Si	75-76	ITEM II Máquinas de Impresión - Ver Sección 1.6 Personalización según el formato y el diseño solicitados
2.2.16	La interfaz del equipo de personalización deberá recibir un XML con los datos a personalizar. Este XML será generado por la plataforma de tarjetas de la JCE y almacenado en un servidor de archivos entre la plataforma y los equipos de personalización. El equipo deberá preparar los datos para realizar la personalización de las credenciales de forma totalmente automática.	Si	67-68	ITEM II Máquinas de Impresión - Ver Sección 1.3 Funcionalidades Informáticas
2.2.17	Además de la interfaz, cada sistema deberá incluir una PC interna con sistema operativo vigente.	Si	71	ITEM II Máquinas de Impresión - Ver Sección 1.3.2 Máquina de Impresión PC Interno
2.2.18	A efectos del desarrollo de aplicaciones de personalización del chip, el fabricante deberá proporcionar un sistema de desarrollo de software. Este sistema incluirá todos los elementos hardware y software necesarios para desarrollar, compilar, depurar y probar las aplicaciones de personalización en un entorno de pruebas completamente aislado de la máquina de producción real. Los elementos de software deberán ser: un SDK de desarrollo con los plug-ins, librerías o módulos adecuados para desarrollar aplicaciones de personalización del chip (para ser utilizado por la JCE o terceros).	Si	77-79	ITEM II Máquinas de Impresión - Ver Sección 1.7 Sistema de desarrollo de software
2.2.19	Además del sistema de desarrollo y emulación descrito anteriormente, el fabricante proporcionará toda la documentación necesaria, incluidos ejemplos descriptivos funcionales, para facilitar el desarrollo de estas aplicaciones a desarrolladores entrenados.	Si	77-79	ITEM II Máquinas de Impresión - Ver Sección 1.7 Sistema de desarrollo de software
2.2.20	En el caso de que el fabricante proporcione la aplicación de personalización del chip deberá ser plenamente funcional tanto en la máquina de producción real como en el entorno de desarrollo. La nueva impresora tendrá un SDK (Software Development Kit) para que se pueda integrar con el sistema de captura de datos de la JCE.	Si	79-3	Entregables Máquinas de Impresión
2.2.21	Los sistemas de personalización deben estar equipados con el software interno de gestión de datos, que proporciona interfaces de usuario claras e iguales para la integración en la red del proyecto. El equipo deberá preparar los datos para realizar la personalización de las credenciales de forma totalmente automática.	Si	65-66 68-69	ITEM II Máquinas de Impresión - Ver Sección 1.2 Sistema de control de máquina de impresión Mühlbauer MCES 1.3.1 1.3.1.Personalización Interfaz del sistema de la máquina de impresión (Preparación de datos, incoherencia, firma de documentos, función de gestión de claves)
2.2.22	El sistema de personalización debe ser capaz de imprimir medidas de seguridad definidas en este pliego. Deberá contar con medidas de seguridad Nivel 1, Nivel 2 y Nivel 3. Especificar qué medidas puede proporcionar en la personalización.	Si	63	ITEM II Máquinas de Impresión - Ver Sección 1.1.5 Sistema láser

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo

2.2.23	Se incluirá la generación de informes de producción, a definir por el organismo (por ejemplo, informes de la producción de un determinado DNI, informes de la producción por máquina -cantidad y detalle de CI y CIE-, o informes de la producción en un periodo de tiempo definido por el usuario en una determinada máquina -cantidad y detalle de CI y CIE -). En cada sistema de personalización se debe crear y almacenar información histórica de listas de trabajos y estadísticas de producción durante un periodo de al menos cuatro semanas.	Si	69-70	ITEM II Máquinas de Impresión - Ver Sección 1.3.1 Apoyo a la presentación de informes
3	**Especificiones Tecnicas de la PKI -CA**			
3.1	**Características generales PKI**	Seleccionar		
3.1.1	PKI para seguridad: En el caso de documentos electrónicos, la PKI se utiliza principalmente para garantizar la autenticidad del documento electrónico y la integridad de los datos almacenados en el chip del mismo. Esto implica verificar la autenticidad del documento electrónico, así como garantizar que los datos no hayan sido modificados desde su emisión.	Si	99 103 104-105 134-135 138 140 139 141	ITEM III Especificaciones Técnicas de la PKI CA y PKI Grabado Chip: Secciones. A. PKI CA. 1.11 Autoridad Subordinada Operativa Ciudadana 1.14.2 Beneficios Generales de la PKI. 1.15.1 Proceso de Integración de la Firma Digital con Llaves en Smartcard: B. Ver sección PKI Identidad Física y Digital en la Descripción del sistema PKI, 2.3.1Autenticación pasiva PKI, 2.4.1Autoridad de certificación con firma de país (CSCA), 2.5.1 1.5.1Autoridad de certificación con firma de país (CSCA) 2.3.3 Firma digital PKI, 2.4.3 Firma digital PKI , 2.5.3 Firma digital PKI
3.1.2	PKI para Firma Digital: La PKI utilizada para la firma digital se utiliza para garantizar la autenticidad, integridad y no repudio de documentos electrónicos. Se utiliza para firmar electrónicamente documentos como contratos, formularios, transacciones financieras, entre otros. El objetivo es proporcionar una forma segura de verificar la identidad del firmante y asegurar que el documento no haya sido alterado después de ser firmado. El vencimiento del certificado digital será estipulado dando cumpliento con la Ley de Comercio Electronico nacional y su reglamento.	Si	90-92 110-117 136-137 139 141-142	ITEM III Especificaciones Técnicas de la PKI CA y PKI Grabado Chip: Secciones: A. Sección PKI CA: 1.7Características de la PKI propuesta 1.21Anexos a Solución PKI 1.21.1Descripción técnica funcional de productos PKI. B. Sección PKI Identidad Física y Digitla Descripción del sistema PKI, 2.3.3 Firma Digital PKI, 2.4.3Servidor de estado de certificados, 2.5.3 Firma Digital PKI
3.1.3	La "PKI de Firma Digital" debe tener su propia cadena de confianza completa, y respectivamente para sus niveles debe estar en línea o fuera de línea. La PKI que emitirá certificados y permitirá firmar documentos a los ciudadanos (PKI ciudadana) debe prever implementar 2 tipos de Autoridades certificadoras (AC): a) la AC raíz, que será la AC del JCE y se empleará únicamente para emitir certificados de ACs subordinadas (operativas); b) La AC subordinada u operativa se encargará de emitir los certificados a los ciudadanos. Asimismo, se precisa que la PKI ciudadana no requiere compatibilidad con ICAO, debido a que su uso será para firmar en aplicaciones de la JCE o comerciales de terceros.		104-105 136-137 139 141-142	ITEM III Especificaciones Técnicas de la PKI CA y PKI Grabado Chip: A. Sección PKI CA: 1.15.1Proceso de Integración de la Firma Digital con Llaves en Smartcard Descripción del sistema PKI B. Sección PKI Identidad Física y Digital 2.3.3, Fima Digital PKI 2.4.3, Firma Digital PKI 2.5.3 Firma Digital
3.1.4	La "PKI de Firma Digital" debe ser una infraestructura independiente que permita la firma electrónica de los Documentos de Identificación electrónicos siguiendo las recomendaciones del Doc 9303 de la OACI para los mecanismos de acceso de Control de Acceso Básico (BAC), Control de Acceso Suplementario con el Protocolo de Establecimiento de Conexión con Contraseña (SAC-PACE). Debe proveerse de los APIS y web Services necesarios para su integración a aplicaciones de la JCE.	Si	104-105 136-137 139 141-142	ITEM III Especificaciones Técnicas de la PKI CA y PKI Grabado Chip: A. Sección PKI CA: 1.15.1Proceso de Integración de la Firma Digital con Llaves en Smartcard Descripción del sistema PKI B. Sección PKI Identidad Física y Digital 2.3.3, Fima Digital PKI 2.4.3, Firma Digital PKI 2.5.3 Firma Digital

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, D.N.

3.1.5	El proveedor deberá proporcionar un portal para firma de documentos con el estándar ISO 32000-1, además de la integración a las aplicaciones de la JCE que permita firmar con certificados tanto en la cédula de identidad o externos .El portal para Firmar documentos debe manejar al menos tres tipos de roles: 1. Administrador, con todos los permisos, esta figura debe poder generar y/o enrolar Agentes Certificadores; 2. Agente Certificador con permisos para enrolar y/o generar certificados para los usuarios finales o firmantes; 3. Firmante, son los usuarios que podrán firmar los documentos.	Si	121-126	ITEM III Especificaciones Técnicas de la PKI CA y PKI Grabado Chip: A. Sección PKI CA: 1.21.3.Descripción Técnica delMotor de Firma Electrónica (SeguriSign)
3.1.6	La infraestructura de llave publica será utilizada para la emitir los certificados y firmar digitalmente las identidades digitales, y poder asegurar el ciclo de vida de los certificados y las verificaciones de identidad que menciona el estándar ISO 18013-5.	Si	132	ITEM III Especificaciones Técnicas de la PKI CA y PKI Grabado Chip: B. Sección PKI Identidad Física y Digital 2.1. Especificaciones de la PKI (Para la emisión de la identidad física y la identidad digital CI/CIE)
3.1.7	Deberá cumplir con ISO 15408 - Nivel de Garantía de Evaluación de Criterios Comunes (EAL) 4+ o superior.	Si	143	ITEM III Especificaciones Técnicas de la PKI CA y PKI Grabado Chip: B. Sección PKI Identidad Física y Digital 2.6.3Despliegue del Sistema
3.1.8	Para el caso del tamaño de llaves de la Autoridad ciudadada, tanto la Autoridad Raíz como la Autoridad Subordinada deberán tener un tamaño de llaves de 4096 bits. Para el caso de los certificados de usuario (ciudadanos) será de 2048 bits.	Si	110 131 144	ITEM III Especificaciones Técnicas de la PKI CA y PKI Grabado Chip: A. Sección PKI CA: 1.10. Anexos a Solución PKI 1.21. 4. Descripción técnica de Módulo Cryptoserver CP5 SE 500 de Utimaco. Rendimiento Disponible Descripción del sistema PKI B. Sección PKI Identidad Física y Digital 2.7. Hardware y Software del sistema PKI - Utimaco Cryptoserver CP5 Se52 PCIe, CC certificado según EN419221-5
3.1.9	El hardware deberá responder a los requerimientos para implementar la infraestructura de criptografía basada en claves públicas (PKI).	Si	110 131 144	ITEM III Especificaciones Técnicas de la PKI CA y PKI Grabado Chip: A. Sección PKI CA: 1.10. Anexos a Solución PKI 1.21. 4. Descripción técnica de Módulo Cryptoserver CP5 SE 500 de Utimaco. Rendimiento Disponible Descripción del sistema PKI B. Sección PKI Identidad Física y Digital 2.7. Hardware y Software del sistema PKI - Utimaco Cryptoserver CP5 Se52 PCIe, CC certificado según EN419221-5
3.1.10	El oferente deberá incluir en su propuesta, toda la infraestructura física necesaria para la implantación, ejecución y mantenimiento de la PKI, el conjunto de hardware y software en las instalaciones que indique la dirección de informática. El contrato de mantenimiento a cotizar será de dos (2) años. A partir de los dos años, la JCE podrá renovar el mantenimiento con el precio establecido del proveedor de forma anual. Para la solución de la PKI el ambiente productivo debe habilitarse en alta disponibilidad con 2 nodos activos en balanceo de carga, un ambiente de DRP en disponibilidad simple (1 nodo) y un ambiente de desarrollo en disponibilidad simple (1 nodo).	Si	94- 97 217 196	ITEM III Especificaciones Técnicas de la PKI CA y PKI Grabado Chip: A. Sección PKI CA: 1.9. Descripción Funcional de los Componentes de PKI B. Sección PKI Identidad Física y Digital ITEM VI. Parte A - Propuesta Infrastructura Centro de Datos. 1.1. Descripción de la solución propuesta 2. Plan de Soporte y Mantenimiento, página 9.

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

3.1.11	Componentes en premisa: HSM, CA, CSCA, DSCA y KMI	Si	110- 117 136-137 141-143 142-143 220 224 227	ITEM III Especificaciones Técnicas de la PKI CA y PKI Grabado Chip: A. Sección PKI CA: 1.21. Anexos a Solución de PKI 31-38 Descripción del sistema PKI, 57-58 B. Sección PKI Identidad Física y Digital 2.3.3, Firma Digital PKI,63 2.5.3 Firma Digital PKI, 63 2.6. REquisitos no funcionales ITEM VI. Instalación de Centro de Datos: 1.1.1. Centro de Datos Principal, página 6. Módulos Criptográficos 1.1.2. Centro de Datos Alterno, 10. Módulos Criptográficos. 1.2.1. Descripción: Ultimaco Server CP5, página 14
3.1.12	En la Nube (compatible con los servicios en la nube de Azure): CMS, CRL/Protocolo de Estado del Certificadoen Línea, Repositorio PKI, y servicios adicionales no críticos	Si	110-114 136-137 141-142	ITEM III Especificaciones Técnicas de la PKI CA y PKI Grabado Chip: A. Sección PKI CA: 1.21. Anexos a Solución de PKI 31-38 Descripción del sistema PKI, 57-58 B. Sección PKI Identidad Física y Digital 2.5.3 Firma Digital PKI, 62 ITEM VI. Instalación de Centro de Datos:
3.1.13	Tanto la PKI de firma de documentos como la PKI de Firma Digital deben cumplir CC EAL 4+	Si	143	ITEM III Especificaciones Técnicas de la PKI CA y PKI Grabado Chip: A. Sección PKI CA: 2.6. 3R Despliegue del Sistema
3.1.14	HSM debe estar certificado FIPS 140-2 Nivel 2 o superior	Si	86 144 220 224 312-A a 312-B	ITEM III. Especifaciones de la PKI CA y PKI de tarjeta física y digital . A. Sección PKI CA. 1.42. Equipos Criptográfico.7s B. Sección PKI Identidad Física y Digital 2.7. Hardware y Software de la PKI, página 65-66 ITEM VI. Instalación de Centro de Datos: 1.1.1. Centro de Datos Principal, página 6. Módulos Criptográficos 1.1.2. Centro de Datos Alterno, 10. Módulos Criptográficos. 1.2.1. Descripción: Utimaco Server CP5, página 14. Brochure Utimaco
3.1.15	El software deberá responder a los requerimientos para implementar la infraestructura de criptografía basada en claves públicas (PKI) descrita anteriormente, y los respectivos hardware y software requeridos para cargar los firmantes de documentos y los CRL, conforme a las especificaciones funcionales de la OACI establecidas en el Doc. 9303 vigente.	Si	90 98 132 133 134 138 140	ITEM III. Especifaciones de la PKI CA y PKI de tarjeta física y digital . A. Sección PKI CA. 1.7. Características de la PKI Propuesta, página 11. 1.10. Autoridad Certificadora Raíz, página 19 B. Sección PKI Identidad Física y Digital 2.1 Especifiaciones de la PKI para la emisión de la identidad física y digital CI'CIE, 53 2.2 Requisitos del sistema 54 2.3.1 Autenticación Pasiva PKI, 55 2.4.1Autoridad de Certificación con firma de País (CSCA), página 59 2.5.1. Autoridad de Certificación con firma de País (CSCA), página 61

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

3.1.16	CSCA (Country Signing Certificate Authority): Autoridad encargada de firmar certificados para entidades gubernamentales o documentos de importancia nacional.	Si	90 98 132 133 134 138 140	ITEM III. Especifaciones de la PKI CA y PKI de tarjeta física y digital . A. Sección PKI CA. 1.7. Características de la PKI Propuesta, página 11. 1.10. Autoridad Certificadora Raíz, página 19 B. Sección PKI Identidad Física y Digital 2.1 Especifiaciones de la PKI para la emisión de la identidad física y digital CI/CIE, 53 2.2 Requisitos del sistema 54 2.3.1 Autenticación Pasiva PKI, 55 2.4.1Autoridad de Certificación con firma de País (CSCA), página 59 2.5.1. Autoridad de Certificación con firma de País (CSCA), página 61
3.1.17	El CSCA utilizará algoritmos criptográficos actuales y almacenará las claves privadas en un HSM de cualquier fabricante.	Si	90 98 132 133 134 138 140	ITEM III. Especifaciones de la PKI CA y PKI de tarjeta física y digital . A. Sección PKI CA. 1.7. Características de la PKI Propuesta, página 11. 1.10. Autoridad Certificadora Raíz, página 19 B. Sección PKI Identidad Física y Digital 2.1 Especifiaciones de la PKI para la emisión de la identidad física y digital CI/CIE, 53 2.2 Requisitos del sistema 54 2.3.1 Autenticación Pasiva PKI, 55 2.4.1Autoridad de Certificación con firma de País (CSCA), página 59 2.5.1. Autoridad de Certificación con firma de País (CSCA), página 61
3.1.18	El CSCA deberá elaborar una lista de revocación de certificados ICAO 9303.	Si	90 98 132 133 134 138 140	ITEM III. Especifaciones de la PKI CA y PKI de tarjeta física y digital . A. Sección PKI CA. 1.7. Características de la PKI Propuesta, página 11. 1.10. Autoridad Certificadora Raíz, página 19 B. Sección PKI Identidad Física y Digital 2.1 Especifiaciones de la PKI para la emisión de la identidad física y digital CI/CIE, 53 2.2 Requisitos del sistema 54 2.3.1 Autenticación Pasiva PKI, 55 2.4.1Autoridad de Certificación con firma de País (CSCA), página 59 2.5.1. Autoridad de Certificación con firma de País (CSCA), página 61

3.1.19	El CSCA debe trabajar en un entorno sin conexión.	Si	90 98 132 133 134 138 140	ITEM III. Especifaciones de la PKI CA y PKI de tarjeta física y digital . A. Sección PKI CA. 1.7. Características de la PKI Propuesta, página 11. 1.10. Autoridad Certificadora Raíz, página 19 B. Sección PKI Identidad Física y Digital 2.1 Especifiaciones de la PKI para la emisión de la identidad física y digital CI/CIE, 53 2.2 Requisitos del sistema 54 2.3.1 Autenticación Pasiva PKI, 55 2.4.1Autoridad de Certificación con firma de País (CSCA), página 59 2.5.1. Autoridad de Certificación con firma de País (CSCA), página 61
3.1.20	El CSCA utilizará una autenticación multifactorial para el inicio de sesión en la interfaz de administración.	Si	90 98 132 133 134 138 140	ITEM III. Especifaciones de la PKI CA y PKI de tarjeta física y digital . A. Sección PKI CA. 1.7. Características de la PKI Propuesta, página 11. 1.10. Autoridad Certificadora Raíz, página 19 B. Sección PKI Identidad Física y Digital 2.1 Especifiaciones de la PKI para la emisión de la identidad física y digital CI/CIE, 53 2.2 Requisitos del sistema 54 2.3.1 Autenticación Pasiva PKI, 55 2.4.1Autoridad de Certificación con firma de País (CSCA), página 59 2.5.1. Autoridad de Certificación con firma de País (CSCA), página 61
3.1.21	El CSCA será capaz de emitir certificados VDS Signer conformes a la OACI 9303.	Si	90 98 132 133 134 138 140	ITEM III. Especifaciones de la PKI CA y PKI de tarjeta física y digital . A. Sección PKI CA. 1.7. Características de la PKI Propuesta, página 12. B. Sección PKI Identidad Física y Digital 2.1 Especifiaciones de la PKI para la emisión de la identidad física y digital CI/CIE, 53 2.2 Requisitos del sistema 54 2.3.1 Autenticación Pasiva PKI, 55 2.4.1Autoridad de Certificación con firma de País (CSCA), página 59 2.5.1. Autoridad de Certificación con firma de País (CSCA), página 61
3.1.22	El CSCA debería ser capaz de emitir certificados de firmante de lista maestra.	Si	91 140	ITEM III. Especifaciones de la PKI CA y PKI de tarjeta física y digital . A. Sección PKI CA. 1.7. Características de la PKI Propuesta, página 12. 2.5.1. Autoridad de Certificación con firma de País (CSCA), página 61

3.1.23	DS (Document Signer): Entidad específica para la firma de documentos digitales, garantizando su autenticidad e integridad.	Si	91 132 133 134 138 140	ITEM III. Especifaciones de la PKI CA y PKI de tarjeta física y digital . A. Sección PKI CA. 1.7. Características de la PKI Propuesta, página 12. B. Sección PKI Identidad Física y Digital 2.1 Especifiaciones de la PKI para la emisión de la identidad física y digital CI/CIE, 53 2.2 Requisitos del sistema 54 2.3.1 Autenticación Pasiva PKI, 55 2.4.1Autoridad de Certificación con firma de País (CSCA), página 59 2.5.1. Autoridad de Certificación con firma de País (CSCA), página 61
3.1.24	El DS dispondrá de un servicio web SOAP al que llamar para la generación de SOD y creará un SOD conforme a la OACI 9303.	Si	91 132 133 134 138 140	ITEM III. Especifaciones de la PKI CA y PKI de tarjeta física y digital . A. Sección PKI CA. 1.7. Características de la PKI Propuesta, página 12. B. Sección PKI Identidad Física y Digital 2.1 Especifiaciones de la PKI para la emisión de la identidad física y digital CI/CIE, 53 2.2 Requisitos del sistema 54 2.3.1 Autenticación Pasiva PKI, 55 2.4.1Autoridad de Certificación con firma de País (CSCA), página 59 2.5.1. Autoridad de Certificación con firma de País (CSCA), página 61
3.1.25	El DS utilizará algoritmos criptográficos actuales y almacenará las claves privadas en un HSM de cualquier fabricante.	Si	91 132 133 134 138 140	ITEM III. Especifaciones de la PKI CA y PKI de tarjeta física y digital . A. Sección PKI CA. 1.7. Características de la PKI Propuesta, página 12. B. Sección PKI Identidad Física y Digital 2.1 Especifiaciones de la PKI para la emisión de la identidad física y digital CI/CIE, 53 2.2 Requisitos del sistema 54 2.3.1 Autenticación Pasiva PKI, 55 2.4.1Autoridad de Certificación con firma de País (CSCA), página 59 2.5.1. Autoridad de Certificación con firma de País (CSCA), página 61
3.1.26	El DS que deberá utilizar una autenticación multifactorial para el inicio de sesión en la interfaz de administración debería avisar claramente antes de que finalice el tiempo de uso de la clave del certificado actualmente utilizado.	Si	91 132 133 134 138 140	ITEM III. Especifaciones de la PKI CA y PKI de tarjeta física y digital . A. Sección PKI CA. 1.7. Características de la PKI Propuesta, página 12. B. Sección PKI Identidad Física y Digital 2.1 Especifiaciones de la PKI para la emisión de la identidad física y digital CI/CIE, 53 2.2 Requisitos del sistema 54 2.3.1 Autenticación Pasiva PKI, 55 2.4.1Autoridad de Certificación con firma de País (CSCA), página 59 2.5.1. Autoridad de Certificación con firma de País (CSCA), página 61

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo

3.1.27	Se utilizará un DS separado para firmar los DTC para la aplicación Tarjeta Digital de la JCE. Este DS independiente requerirá una interfaz para acceder al sistema back-end de la JCE.	Si	91 132 133 134 138 140	ITEM III. Especifaciones de la PKI CA y PKI de tarjeta física y digital . A. Sección PKI CA. 1.7. Características de la PKI Propuesta, página 12. B. Sección PKI Identidad Física y Digital 2.1 Especifiaciones de la PKI para la emisión de la identidad física y digital CI/CIE. 53 2.2 Requisitos del sistema 54 2.3.1 Autenticación Pasiva PKI, 55 2.4.1Autoridad de Certificación con firma de País (CSCA), página 59 2.5.1. Autoridad de Certificación con firma de País (CSCA), página 61
3.2.	**Autoridad de Certificación (CA) de firma de país (CSCA)**			
3.2.1	El adjudicatario deberá implementar una CA con especificaciones y un marco que deberá cumplir con el Documento 9303 de la OACI vigente sobre el esquema de Firmas Digitales PKI propuesto para autenticar la tarjeta electrónica que ofrece acceso de sólo lectura de Chip de Circuito Integrado (IC).	Si	91 132 133 134 138 140	ITEM III. Especifaciones de la PKI CA y PKI de tarjeta física y digital . A. Sección PKI CA. 1.7. Características de la PKI Propuesta, página 12. B. Sección PKI Identidad Física y Digital 2.1 Especifiaciones de la PKI para la emisión de la identidad física y digital CI/CIE, 53 2.2 Requisitos del sistema 54 2.3.1 Autenticación Pasiva PKI, 55 2.4.1Autoridad de Certificación con firma de País (CSCA), página 59 2.5.1. Autoridad de Certificación con firma de País (CSCA), página 61
3.2.2	El adjudicatario instalará para la JCE, y en las propias instalaciones de la JCE, los sistemas y equipos necesarios para generar conjuntos de claves para diferentes períodos de tiempo que se utilizarán para computar las Firmas Digitales que se aplicarán para la firma de los Certificados	Si	110-117 136-137 141 142-143 225	ITEM III Especificaciones Técnicas de la PKI CA y PKI Grabado Chip: A. Sección PKI CA: 1.21. Anexos a Solución de PKI 31-38 B. Sección PKI Identidad Física y Digital 2.3.3. Firma Digital PKI,57-58 2.5.3 Firma Digital PKI 2.6. REquisitos no funcionales, 64 ITEM VI. Instalación de Centro de Datos: 1.2. Diagrama de la Solución

3.2.3	Los sistemas o instalaciones propuestos deberán estar bien protegidos de cualquier acceso externo o no autorizado a través del diseño inherente y las instalaciones de seguridad de hardware y requerirá medidas de seguridad robustas, entre otras: - Atenticación multifactorial (MFA para acceso a la administración). Cifrado avanzado en todas las comunicaciones y datos almacenados, utilizando algoritmos criptográficos robustos y actuales. - Uso de Módulos de Seguridad por Hardware (HSMs) certificados (FIPS 140-2 nivel 2 o superior) para la generación y almacenamiento de claves privadas. - Implementación de sistemas avanzados de monitoreo y detección de intrusos (IDS/IPS). - El monitoreo debe incluir de infraestructura, de seguridad y de comuniciones - Segmentación de redes que aisle la infraestructura de PKI de otras redes corporativas. - Mantenimiento de todos los sistemas y software de la PKI actualizados con los últimos parches de seguridad. - Realización de auditorías regulares y evaluaciones de seguridad. - Capacitación del personal involucrado en la operación y gestión de la PKI sobre las mejores prácticas de seguridad y procedimientos de respuesta a incidentes.	Si	110 90 126-131 50-52 143 144	ITEM III Especificaciones Técnicas de la PKI CA y PKI Grabado Chip: A. Sección PKI CA: 1.21.1. Anexos a Solución de PKI, 31 1. 7. Características de la PKI Propuesta, página 12. 1.21.4. Descripción técnica de módulo Cryptoserver CP5 SE500 de Utimaco. 48-49 1.21.5 Descripción técnica de módulo Cryptoserver CP5 SE 12 de Utimaco, 50-52 B. Sección PKI Identidad Física y Digital 2.7 . Hardware y software de la PKI
3.2.4	La solución debe de ser redundante y el oferente debe de explicar y detallar cómo. La aplicación de software que implementa CSCA y CVCA se desea que cumplan con el EAL 4+ pero no es obligatorio.	Si	143 217	ITEM III Especificaciones Técnicas de la PKI CA y PKI Grabado Chip: B. Sección PKI Identidad Física y Digital 2.6.3. Despliegue del sistema,64. ITEM VI. Infraestructura de Centro de Datos :1.1. Descripción de la solución propuestas
3.2.5	Es obligatorio implementar planes de recuperación ante desastres y continuidad del negocio para la infraestructura PKI. Es importante que el plan de continuidad y recuperación ante desastres esté alineado con las normas internacionales, como la ISO/IEC 27031, que establece directrices para la preparación en tecnologías de la información, y la ISO 22301, que cubre los sistemas de gestión de continuidad del negocio.		233- 235	ITEM VI. Infraestructura de Centro de Datos 4 Justificación del Plan de Recuperación y Respaldo
3.2.6	El proveedor adjudicado debe de coordinar y apoyar la implementación de la CA con las disposiciones legales establecidas en la Ley 126-02 sobre Comercio Electrónico, Documentos y Firma Digital y su reglamento contenido en el Decreto 335-03. Debe apoyar el proveedor adjudicado con su personal experto, en los pasos a seguir para establecer la CA en el país, y en los documentos que debe de generar. Pero la presentación y la autorización dependerá de la JCE ante las entidades gubernamentales.	Si	109	ITEM III Especificaciones Técnicas de la PKI CA y PKI Grabado Chip: A. Sección PKI CA: 1.20. Entregables del Proyecto, página 28 – 30
3.2.7	Los certificados de CA de firma de país se generarán en una infraestructura de CA sin conexión, altamente protegida. El oferente deberá presentar la infraestructura aportando justificaciones adecuadas para su selección. Es necesaria la compatibilidad en la generación de certificados digitales X509	Si	92 138-139	ITEM III Especificaciones Técnicas de la PKI CA y PKI Grabado Chip: A. Sección PKI CA: 1. 8. Otras consideraciones para la CSCA, página 13. B. Sección PKI Identidad Física y Digital 2.4.1. Autoridad de Certificación con firma de país (CSCA).59 2.4.3. Firma Digital PKI, 59-60
3.2.8	El oferente debe de incluir en su propuesta la inclusión, instalación, configuración y puesta en marcha de un dispositivo HSM certificado con FIPS 140-2 o mayor, que será instalado en las instalaciones de la JCE.eIDAS CC EAL4+ debe ser parte de las características de los HSM. La combinación de eIDAS con la certificación CC EAL4+ se refiere a productos o servicios de identificación electrónica y de confianza que cumplen con los altos estándares de seguridad definidos por Common Criteria y que también cumplen con los requisitos del reglamento eIDAS.	Si	126-131 50-52 143 144	ITEM III Especificaciones Técnicas de la PKI CA y PKI Grabado Chip: A. Sección PKI CA: 1. 21.4. Descripción Técnica Módulo Criptoserver, página 47. 1.21.5 Descripción técnica de Módulo Criptoserver CP5SE 12 de Utimaco, página 50 B. Sección PKI Identidad Física y Digital 2.6.3. Despliegue del Sistema, página 64 2.7. Hardware y Software del Sistema PKI, página 65

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

3.2.9	La PKI que emitirá certificados y permitirá firmar documentos a los ciudadanos (PKI ciudadana) debe prever implementar 2 tipos de Autoridades certificadoras (AC): a) la AC raíz, que será la AC del JCE y se empleará únicamente para emitir certificados de ACs subordinadas (operativas); b) La AC subordinada u operativa se encargará de emitir los certificados a los ciudadanos.	Si	83-145	ITEM III Especificaciones Técnicas de la PKI CA A. Sección PKI CA: página 4-66
3.2.10	**APIS criptográficos (podrá soportar)**			
3.2.10.1	PCKCS#11	Si	312-A a 312-B	Brochure Utimaco_CC_eIDAS_Datasheet
3.2.10.2	Java	Si	125 143	ITEM III Especificaciones Técnicas de la PKI CA y PKI Grabado Chip: A. Sección PKI CA: 1.21.3 Descripción Técnica de Motor de Firma Electrónica, página 46 (Interfaz de Desarrollo) B. Sección PKI Identidad Física y Digital 2.6.3. Despliegue del Sistema, página 64
3.2.10.3	Microsoft CAPI y CNG	Si	143	ITEM III Especificaciones Técnicas de la PKI CA y PKI Grabado Chip: A. Sección PKI CA: 1.21.3 Descripción Técnica de Motor de Firma Electrónica, página 46 (Interfaz de Desarrollo) Utimaco_CC_eIDAS_Datasheet
3.2.10.4	OpenSSL.	Si	111-114	ITEM III Especificaciones Técnicas de la PKI CA y PKI Grabado Chip: A. Sección PKI CA: 1.21.3 Descripción Técnica Funcional de Produtos de PKI, página 31 - 35 (incluyendo Interfaz Web)
3.2.11	**Algoritmos criptográficos asimétricos (podrá soportar)**			
3.2.11.1	RSA	Si	312-A a 312-B	UTIMACO CC_eIDAS Ficha Técnica
3.2.11.2	DSA	Si	312-A a 312-B	UTIMACO CC_eIDAS Ficha Técnica
3.2.11.3	ECC	Si	312-A a 312-B	UTIMACO CC_eIDAS Ficha Técnica
3.2.11.4	ECDSA	Si	312-A a 312-B	UTIMACO CC_eIDAS Ficha Técnica
3.2.11.5	ECDH	Si	312-A a 312-B	UTIMACO CC_eIDAS Ficha Técnica
3.2.11.6	Ed25519	Si	312-A a 312-B	UTIMACO CC_eIDAS Ficha Técnica
3.2.11.7	ECIES	Si	312-A a 312-B	UTIMACO CC_eIDAS Ficha Técnica
3.2.11.8	Brainpool curves (nombrados y definidos por el usuario)	Si	312-A a 312-B	UTIMACO CC_eIDAS Ficha Técnica
3.2.11.9	Diffie Hellman (DH)	Si	312-A a 312-B	UTIMACO CC_eIDAS Ficha Técnica
3.2.12	**Algoritmos criptográficos simétricos (podrá soportar)**	Si	312-A a 312-B	UTIMACO CC_eIDAS Ficha Técnica
3.2.12.1	AES			
3.2.12.2	AES-GCM	Si	312-A a 312-B	UTIMACO CC_eIDAS Ficha Técnica
3.2.12.3	DES	Si	312-A a 312-B	UTIMACO CC_eIDAS Ficha Técnica
3.2.12.4	3DES	Si	312-A a 312-B	UTIMACO CC_eIDAS Ficha Técnica
3.2.12.5	ARIA	Si	312-A a 312-B	UTIMACO CC_eIDAS Ficha Técnica
3.2.12.6	SEED	Si	312-A a 312-B	UTIMACO CC_eIDAS Ficha Técnica
3.2.12.7	RC2	Si	312-A a 312-B	UTIMACO CC_eIDAS Ficha Técnica
3.2.12.8	RC4	Si	312-A a 312-B	UTIMACO CC_eIDAS Ficha Técnica
3.2.12.9	RC5	Si	312-A a 312-B	UTIMACO CC_eIDAS Ficha Técnica
3.2.12.10	CAST	Si	312-A a 312-B	UTIMACO CC_eIDAS Ficha Técnica
3.2.13	**Condiciones de Operación**			
3.2.13.1	Voltajes de operación: 110/220 V.	Si	312-A a 312-B	UTIMACO CC_eIDAS Ficha Técnica
3.2.13.2	Temperatura de operación: 10°C- 40°C.	Si	312-A a 312-B	UTIMACO CC_eIDAS Ficha Técnica
3.2.13.3	Humedad relativa no condensada: 20% a 90%	Si	312-A a 312-B	UTIMACO CC_eIDAS Ficha Técnica
3.2.13.4	MTBF mínimo 150,000 horas a 25°C /77°F	Si	312-A a 312-B	UTIMACO CC_eIDAS Ficha Técnica
3.2.14	**Certificaciones de seguridad**		312-A a 312-B	

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

3.2.14.1	FIPS 140-2 Nivel 2 o superior – Password and Multi-Factor (PED)	Si	312-A a 312-B	UTIMACO CC_eIDAS Ficha Técnica
3.2.14.2	eIDAS CC EAL4+	Si	312-A a 312-B	UTIMACO CC_eIDAS Ficha Técnica
3.2.15	**Características generales**			
3.2.15.1	Generación de números aleatorios reales (TNRG)	Si	312-A a 312-B	UTIMACO CC_eIDAS Ficha Técnica
3.2.15.2	Copia de seguridad de la inteligente del material clave	Si	312-A a 312-B	UTIMACO CC_eIDAS Ficha Técnica
3.2.15.3	Doble conector de red	Si	312-A a 312-B	UTIMACO CC_eIDAS Ficha Técnica
3.2.15.4	Administración remota (vía red)	Si	312-A a 312-B	UTIMACO CC_eIDAS Ficha Técnica
3.2.15.5	Administración local	Si	312-A a 312-B	UTIMACO CC_eIDAS Ficha Técnica
3.2.15.6	Soportar interface gráfica del HSM	Si	312-A a 312-B	UTIMACO CC_eIDAS Ficha Técnica
3.2.15.7	Opciones múltiples para autentificación y control de acceso.	Si	312-A a 312-B	UTIMACO CC_eIDAS Ficha Técnica
3.2.15.8	Múltiple integración para aplicaciones de PKI, servicios de encriptación	Si	312-A a 312-B	UTIMACO CC_eIDAS Ficha Técnica
3.2.15.9	Separación de tareas	Si	312-A a 312-B	UTIMACO CC_eIDAS Ficha Técnica
3.2.15.10	Sistemas operativos soportados: Windows y Linux	Si	312-A a 312-B	UTIMACO CC_eIDAS Ficha Técnica
3.2.15.11	Rendimiento nominal mínimo (firmas RSA /segundo, 2048 bit, modo Bulk): 25	Si	312-A a 312-B	UTIMACO CC_eIDAS Ficha Técnica
3.2.15.12	Habilitado para operación en cluster (alta disponibilidad).	Si	312-A a 312-B	UTIMACO CC_eIDAS Ficha Técnica
3.2.15.13	Debe permitir la importación /exportación de llaves internas a través de un método seguro, desde y hacia otro HSM.	Si	312-A a 312-B	UTIMACO CC_eIDAS Ficha Técnica
3.2.15.14	El HSM deberá proveer mecanismos de detección de apertura llamados "Tamper Evidence" y ser resistentes al forzado, característica denominada "Intrusion Resistant".	Si	312-A a 312-B	UTIMACO CC_eIDAS Ficha Técnica
4	**Especificaciones de la Tarjeta de Identidad Digital**			
4.1	Certificación: La solución ofrecida debe contar con la certificación ISO/IEC 18013 Parte 5.	Si	148	ITEM IV Propuesta Técnica para la Tarjeta de Identidad Digital - ver sección 1.1 Resumen de la solución
4.2	Estar preparada para cumplir con el estándar de la OACI ("Guiding Core Principles for the Development of Digital Travel Credential (DTC) de octubre de 2020"	Si	152-153	ITEM IV Propuesa Técnica para la Tarjeta de Identidad Digital - ver sección 1.4 Arquitectura de confianza cero - Consideraciones adicionales
4.3	El oferente deberá implementar la solución de identidad digital antes de 26 SEMANAS tras la firma del contrato	Si	789-B 789-1	Ver Documento Detalle del Cronograma Cumplimiento, ETAPA 1:IMPLANTACIÓN Y PUESTA EN MARCHA DEL PROYECTO, # 6 Realizar las pruebas piloto de la solución digital de la tarjeta CD (Mobile ID) antes de veintiséis (26) semanas, incluyendo el desarrollo de una app para la JCE. Semana 20. Actividad 249: Pruebas (789_I)
4.4	Será administrado por la JCE integrada a su vez al sistema nacional de identidad mediante el uso de APIS que tendrían que ser desarrollados por oferente adjudicado. Las bases de datos actuales del sistema de cedulación está en SQL server 2022, la arquitectura es cliente servidor.	Si	149-152	ITEM IV Propuesta Técnica para la Tarjeta de Identidad Digital - ver sección 1.2 Plataforma de microservicios de identificación digital - Gestión de identidades y accesos
4.5	Los datos entregados deberán ser firmados electrónicamente. Esta firma electrónica certificada de los datos permitirá que terceros puedan validar la integridad y procedencia de los datos que presenta el ciudadano. Los datos entregados deberán ser firmados electrónicamente por la JCE. Esta firma electrónica certificada de los datos permitirá que terceros puedan validar la integridad y procedencia de los datos que presenta el ciudadano, tanto la firma de los datos como la validación de estos, se realizará usando los certificados electrónicos administrados por la JCE, como Autoridad Certificadora descrita en el apartado Infraestructura de clave pública.	Si	174	ITEM IV Propuesta Técnica para la Tarjeta de Identidad Digital - ver sección Anexo - Apéndice 1 - Visión general de la arquitectura:
4.6	La aplicación deberá demostrar un código bidimensional con los datos y su respectiva firma electrónica certificada. La aplicación debe permitir al usuario seleccionar la lista de campos que desee compartir a través del código bidimensional.	Si	178-4	ITEM IV Propuesta Técnica para la Tarjeta de Identidad Digital - ver sección 1.7 Expeeriencia de usuario y autoservicio - Billetera Digital: ver ITEM IV VeriGo MobileID – Anexo Casos de Uso - sección 2 Privacidad
4.7	**Aspectos generales de la Tarjeta Digital**			
4.7.1	La solución debe incluir el sistema de gestión del ciclo de vida de las credenciales digitales (emisión, activación y revocación), de forma que se registren los eventos de acceso a cada credencial, así como proporcionar las aplicaciones o interfaces necesarias para la implantación de nuevas soluciones. El ciclo de vida debe ser emisión, activación, revocación.	Si	149	ITEM IV Propuesta Técnica para la Tarjeta de Identidad Digital - ver sección 1.2 Plataforma de microservicios de identificación digital - Emisión de tarjetas de identidad digital (CD) y gestión de perfiles de usuario

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

4.7.2	El cuidadano debe tener acceso a un portal donde pueda actualizar sus credenciales, cancelarlas, inspeccionar los accesos a su identidad. La solucion debe permitir al ciudadano el acceso a un portal donde pueda actualizar sus credenciales, cancelar su aplicación, inspeccionar los accesos a su identidad y en general observar todas las transacciones que ha realizado con la misma. Se deben poder validar todas las operaciones realizadas con su identidad incluyendo la fecha y hora de las mismas. Debe tener la capacidad de mostrar el tipo de acceso aun si es hecho desde aplicaciones de terceros. Deben gestionarse todos los eventos del ciclo de vida y consultas.	Si	150-151	ITEM IV Propuesta Técnica para la Tarjeta de Identidad Digital - ver sección 1.2 Plataforma de microservicios de identificación digital - Creación y modificación de usuarios
4.7.3	El proveedor deberá monitorizar todos los sistemas 24x7	Si	240-241	ITEM VI Infraestructura de Centro de Datos - ver sección 6. Premisas y Entregables
4.7.4	La solución debe disponer de un canal de comunicación que utilice algoritmos de cifrado, como medio de conexión entre los dispositivos, para ejecutar el proceso de verificación. El uso de diferentes transmisiones debe incluir los protocolos NFC (Near Field Communication) y BLE (Bluetooth Low Energy) y el cumplimiento de la norma ISO 18013-5.	Si	160-162	ITEM IV Propuesta Técnica para la Tarjeta de Identidad Digital - ver sección 2.2 Normas de seguridad de la plataforma
4.7.5	La solución debe tener las funciones de recepción, almacenamiento y protección segura de credenciales digitales en aplicaciones móviles, así como el uso de notificaciones PUSH para enviar mensajes masivos o personalizados al titular de la credencial digital. Se espera enviar notificaciones personales por actualización de datos, o notificaciones masivas relacionadas a las acciones de JCE.	Si	161-162	ITEM IV Propuesta Técnica para la Tarjeta de Identidad Digital - ver sección 1.2 Plataforma de microservicios de identificación digital - Alertas y notificaciones
4.7.6	La solución debe utilizar durante el proceso de emisión o activación de la identidad digital, el mecanismo de detección de liveness (prueba de vida), para prevenir ataques de presentación. La solución debe de cumplir con el ISO 30107-3.	Si	154	ITEM IV Propuesta Técnica para la Tarjeta de Identidad Digital - ver sección 1.5 Verificación y validación de la identidad - Verificación de la prueba de identidad
4.7.7	Las aplicaciones móviles deberán proporcionar al titular del documento de identidad digital el desbloqueo de la App mediante autenticación de dos factores (2FA), al menos el uso de un PIN y/o verificación facial.	Si	154	ITEM IV Propuesta Técnica para la Tarjeta de Identidad Digital - ver sección 1.5 Verificación y validación de la identidad - Autenticación biométrica
4.7.8	Las aplicaciones móviles tendrán que funcionar sin conexión, para permitir la visualización local de los datos de las credenciales digitales, utilizando un método de verificación de la autenticidad de la identidad digital. También deberá tener la capacidad de realizar consultas en línea, en caso de que se requiera llevar a cabo algún tipo de verificación de la información del titular de la identidad digital. Se espera que la app permita a alguien con la aplicación de verificación validar la identidad del ciudadano por medio de la lectura de los datos almacenados en el dispositivo. Se debe poder validar la identidad por medio de una app de verificación tal como se ha especificado o bien desde otros dispositivos tipo PC que puedan leer los QR o bien lectores de RFID.	Si	156-157	ITEM IV Propuesta Técnica para la Tarjeta de Identidad Digital - ver sección 1.7 Experiencia de usuario y autoservicio - Billetera Digital
4.7.9	Las aplicaciones móviles deben permitir la visualización del documento de identidad digital, preferiblemente en modo de pantalla completa del dispositivo móvil, cambiando de anverso a reverso al tocar la credencial y mostrando los mismos datos del documento de identidad físico.	Si	156-157	ITEM IV Propuesta Técnica para la Tarjeta de Identidad Digital - ver sección 1.7 Experiencia de usuario y autoservicio - Billetera Digital
4.7.10	Las aplicaciones móviles deben tener la capacidad de compartir únicamente la información que el titular de la identidad digital desee compartir, en el momento de la verificación de la identidad, al menos: nombre completo, número de cédula de identidad, fecha de nacimiento, fecha de vencimiento de la cédula de identidad, sexo. En la app del ciudadano debe darle la opción de marcar cuales de los datos desea compartir con la persona que está haciendo la verificación.	Si	158	ITEM IV Propuesta Técnica para la Tarjeta de Identidad Digital - ver sección 1.7 Experiencia de usuario y autoservicio - Verificador Móvil
4.7.11	Las aplicaciones móviles deben informar al titular cuando su identidad digital ha sido revocada, mediante una alerta al entrar en la App, indicando el cambio en la validez de su documento digital. La identidad digital poder ser revocada por el ciudadano en el portal de identidad digital usando su user y clave de acceso o bien por medio del portal ciudadano por una autoridad competente de la JCE.	Si	151-152	ITEM IV Propuesta Técnica para la Tarjeta de Identidad Digital - ver sección 1.2 Plataforma de microservicios de identificación digital - Alertas y notificaciones

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo R.D.

4.7.12	La solución debe ser modular, escalable y fácilmente optimizable para adaptarse a la evolución de la demanda de este tipo de documentos. Se definirán las KPI una vez se adjudique el contrato. La escalabilidad debe permitir el volumen de credenciales digitales que es estimado en 800 mil en dos años	Si	159-171 232	ITEM IV Propuesta Técnica para la Tarjeta de Identidad Digital - ver sección 2 Arquitectura del sistema Referencia: ITEM VI. Propuesta Infraestructura Centro de Datos, punto 3. Justificación, Base de Datos, unidad de Almacenamiento
4.7.13	La solución debe incluir mecanismos de hardening y protección contra ataques que incluyan, entre otros, ingeniería inversa, manipulación de código, detección de rooting/jailbreak/debugging, etc.	Si	156-157	ITEM IV Propuesta Técnica para la Tarjeta de Identidad Digital - ver sección 1.7 Experiencia de usuario y autoservicio - Billetera Digital
4.7.14	La solución debe poseer la capacidad de incorporar información en las imágenes de los solicitantes como medidas de seguridad complementarias.	Si	156-157	ITEM IV Propuesta Técnica para la Tarjeta de Identidad Digital - ver sección 1.7 Experiencia de usuario y autoservicio - Billetera Digital
4.7.15	El proveedor de la solución debe haber realizado con éxito un mínimo de un proyecto de identidad digital de 100 mill credenciales (es válido con empresas del mismo grupo económico)	Si	845-848	Experiencia en distintos clientes y países, en cédulas digital o identidades móviles (Mobile ID)
4.7.16	Herramientas de Desarrollo: Facilitar SDK y API. Uso por personal técnico o terceros. Los SDK y APIS deben facilitar las tareas de integración que deberá implementar la JCE para la emisión, control, actualización u otras acciones que se requieran realizar en relación a la Tarjeta Digital	Si	155-159	ITEM IV Propuesta Técnica para la Tarjeta de Identidad Digital - ver sección 1.7 Experiencia de usuario y autoservicio
4.7.17	El oferente debe presentar un plan de integración con los sistemas de identificación JCE. Se debe integrar el Sistema de Enrolamiento y emision de cedulas de identidad y sus sistemas relacionados	Si	175	ITEM IV Propuesta Técnica para la Tarjeta de Identidad Digital - ver sección Anexo - Apéndice 1 - Integración con el sistema heredado JCE
4.7.18	Infraestructura PKI: la solución debe implementar infraestructura PKI para emisión de certificados. El oferente debe presentar las especificaciones de la infraestructura PKI ofrecida.	Si	92-93	ITEM III Especificaciones Técnicas de la PKI CA 1.8Especificaciones técnicas tarjeta de identidad digital y la Autoridad Certificadora
4.7.19	Aplicaciones Móviles: La solución debe incluir la implementación de aplicaciones móviles multiplataforma compatibles con iOS y Android. El oferente debe presentar el plan de implementación de aplicaciones móviles.	Si	148	ITEM IV Propuesta Técnica para la Tarjeta de Identidad Digital - ver sección 1.1 Resumen de la solución
4.7.20	Seguridad: La solución debe incluir Protección contra ingeniería inversa y clonación. El oferente debe presentar los mecanismos de seguridad implementados.	Si	156-157	ITEM IV Propuesta Técnica para la Tarjeta de Identidad Digital - ver sección 1.7 Experiencia de usuario y autoservicio - Billetera Digital
4.7.21	Activación Remota: La solución debe incluir un mecanismo para activación remota de identidad digital, debe considerarse el tiempo de validez del enlace. El oferente debe describir el proceso de activación con enlace. El enlace debe poderse enviar por correo electronico o bien por medio de mensaje de texto o por otro medio a determinar. Se debe manejar doble factor de autenticacion 2FA y los enlaces no deben ser validos por más de unas horas.	Si	148 150-151	ITEM IV Propuesta Técnica para la Tarjeta de Identidad Digital - ver sección 1.1 Resumen de la solución ver Gestión del ciclo de vida del DNI digital - Creación y modificación de usuarios
4.7.22	Liveness Detection: La solución debe utilizar liveness detección para el proceso de activación de identidad digital remota para la Prevención de suplantación de identidad de acuerdo con el estándar de referencia: ISO 30107-3. El oferente deberá presentar la Certificación de cumplimiento de ISO 30107-3.	Si	178-3	ITEM IV VeriGo MobileID – ver Anexo Casos de Uso - sección 1 Prueba de vida
4.7.23	Alta Disponibilidad: La plataforma debe contar con un esquema de alta disponibilidad de servicio. Debe garantizar la continuidad del servicio de manera interrumpida. La Plataforma debe poder adecuarse al esquema de alta disponibilidad instalado en nuestro site alterno. Eso implica un tiempo de inactividad de no más de cinco minutos antes de que el servicio sea transferido al site alterno. Este site alterno cuenta con una infraestructura que garantiza un almacenamiento y un hardware que permite ejecutar al menos los servicios principales sin pérdida de datos al realizar el failover.	Si	164-166	ITEM IV Propuesta Técnica para la Tarjeta de Identidad Digital - ver sección 2.5. Método de despliegue: Multi-Host On-Premise - Contenedores Docker - Modelos de infraestructura
4.7.24	Interoperabilidad: La plataforma debe permitir la interoperabilidad y escalabilidad del servicio. El oferente debe presentar la descripción de módulos o componentes.	Si	174	ITEM IV Propuesta Técnica para la Tarjeta de Identidad Digital - ver sección Anexo - Apéndice 1 - Diagrama de la plataforma de identificación móvil

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

4.7.25	Intercambio de Datos: La aplicación de identidad móvil debe permitir intercambio de datos personales iniciado por el titular de acuerdo con la norma ISO/IEC 18013-5. El oferente debe demostrar los Métodos de intercambio (QR, NFC, Bluetooth). El código QR es requerido para la vinculación de los dispositivos y el intercambio de datos se realizará utilizando al menos un método entre NFC o BLE.	Si	156-157	ITEM IV Propuesta Técnica para la Tarjeta de Identidad Digital - ver sección 1.7 Experiencia de usuario y autoservicio - Billetera Digital
4.7.26	Selección de Datos: La aplicación de identidad móvil debe permitir selección de campos especificos para compartir y las Categorías de campos. El oferente debe demostrar la Funcionalidad de selección en la aplicación a implementar.	Si	156-157	ITEM IV Propuesta Técnica para la Tarjeta de Identidad Digital - ver sección 1.7 Experiencia de usuario y autoservicio - Billetera Digital
4.7.27	Administración de Emisiones: La solución debe Incluir el sistema para administración de la emisión de identidades digitales para evidenciar el registro de eventos y accesos incluir las interfaces necesarias para nuevas soluciones. Se deben registrar al menos todos los eventos donde la identidad es consultada o verificada, los accesos y acciones del ciudadano en el portal de gestion y los relacionados a intentos fallidos de acceso.	Si	156-157	ITEM IV Propuesta Técnica para la Tarjeta de Identidad Digital - ver sección 1.7 Experiencia de usuario y autoservicio - Billetera Digital
4.7.28	Seguridad de Comunicaciones: Asegurar todas las comunicaciones entre aplicaciones móviles, incluyendo las interacciones en línea y fuera de línea. El oferente debe demostrar los Mecanismos de seguridad de comunicación.	Si	160-162	ITEM IV Propuesta Técnica para la Tarjeta de Identidad Digital - ver sección 2.2 Normas de seguridad de la plataforma
4.7.29	Canales de Comunicación: Utilizar algoritmos de encriptación en canales de comunicación. Se deben incluir las especificaciones de algoritmos utilizados. Se requiere al menos el uso de protocolos NFC y BLE.	Si	160-162	ITEM IV Propuesta Técnica para la Tarjeta de Identidad Digital - ver sección 2.2 Normas de seguridad de la plataforma
4.7.30	Funcionalidades de App: La solución deberá proveer las Funciones para recibir, guardar y proteger credenciales digitales. Se debe demostrar el uso de Notificaciones PUSH y almacenamiento seguro. Se espera enviar notificaciones personales por actualizacion de datos, o notificaciones masivas relacionadas a las acciones de JCE.	Si	151-152	ITEM IV Propuesta Técnica para la Tarjeta de Identidad Digital - ver sección 1.2 Plataforma de microservicios de identificación digital - Alertas y notificaciones
4.7.31	Autenticación: Las aplicaciones móviles deberán permitir el desbloqueo de la App mediante autenticación de dos factores 2FA, como mínimo PIN y verificación facial.	Si	150-151	ITEM IV Propuesta Técnica para la Tarjeta de Identidad Digital - Gestión del ciclo de vida del DNI digital - Creación y modificación de usuarios
4.7.32	Funcionalidad Online / Offline: Las aplicaciones móviles deberán permitir el funcionamiento offline para visualización de datos Debe permitir también las Consultas en línea. Lo que se espera es que el app permita a alguien con la aplicación de verificacion validar la identidad del ciudadano por medio de la lectura de los datos almacenados en el dispositivo.	Si	156-157	ITEM IV Propuesta Técnica para la Tarjeta de Identidad Digital - ver sección 1.7 Experiencia de usuario y autoservicio - Billetera Digital
4.7.33	Visualización de Documentos: Visualización de documentos de identificación digital en pantalla completa y el cambio de anverso a reverso. El diseño final de la identidad movil sera acordada con el adjudicatario.	Si	156	ITEM IV Propuesta Técnica para la Tarjeta de Identidad Digital - ver sección 1.7 Experiencia de usuario y autoservicio - Billetera Digital
4.7.34	Compartir Información: Capacidad de compartir información seleccionada durante verificación de identidad.	Si	158	ITEM IV Propuesta Técnica para la Tarjeta de Identidad Digital - ver sección 1.7 Experiencia de usuario y autoservicio - Verificador Móvil
4.7.35	Notificaciones de Revocación: Informar al titular sobre la revocación de su identidad digital mediante alertas en la App. Se debe poder notificar al menos por medio de correo electronico y mensajes SMS de telefono celular. u otro medio a designar.	Si	151-152	ITEM IV Propuesta Técnica para la Tarjeta de Identidad Digital - ver sección 1.2 Plataforma de microservicios de identificación digital - Alertas y notificaciones
4.7.36	Capacidad de Servicio: Atender al menos 5,000 solicitudes diarias de credenciales digitales. La solución debe ser Modular y escalable para adaptarse a la evolución en la demanda de este tipo de documentos. El oferente deberá proporcionar información de dimensionamiento de la plataforma.	Si	164-166	ITEM IV Propuesta Técnica para la Tarjeta de Identidad Digital - ver sección 2.5. Método de despliegue: Multi-Host On-Premise - Contenedores Docker - Modelos de infraestructura
4.7.37	Interfaces de Comunicación: Utilizar e integrar con interfaces de comunicación existentes para el envio de orden de emisión por parte de la JCE.	Si	170-173	ITEM IV Propuesta Técnica para la Tarjeta de Identidad Digital - ver sección 2.8. Análisis de interfaces y plan de pruebas para interfaces de comunicación
4.7.38	Análisis de Interfaces: Se deberá presentar un plan de análisis y pruebas para el ajuste de interfaces de comunicación propuestas por el JCE. Se deben incluir igualmente a definición de escenarios de prueba.	Si	170-178	ITEM IV Propuesta Técnica para la Tarjeta de Identidad Digital - ver sección 2.8. Análisis de interfaces y plan de pruebas para interfaces de comunicación
4.7.39	Consistencia de Datos: Mantener consistencia de estados entre soluciones para el Proceso de actualización y sincronización al sistema institucional para la identificación de personas.	Si	233-235	ITEM VI Propuesta Infraestructura de Centro de Datos - ver sección 4. Justificación del Plan de Recuperación y Respaldo

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

4.7.40	Disponibilidad de operación: Disponibilidad del 99.95% durante horas de producción, excepto por razones atribuibles a la JCE. El oferente deberá presentar un Plan de operación y mantenimiento.	Si	190 217	ITEM VI PARTE B Especificaciones Técnicas del Mantenimiento o SLA, ver1.1. VI.1 Especificaciones técnicas del Mantenimiento ITEM VI PARTE A ver 1.1. VI.1 Infraestructura Centro de Datos, 1. Equipos Activos de la Solución Propuesta - 1.1 Descripción de la solución propuesta
4.7.41	Es aceptable para la entidad que la solución de identidad digital se despliegue en la nube.	Si	148 175-176	ITEM IV Propuesta Técnica para la Tarjeta de Identidad Digital - ver sección 1.1 Resumen de la solución ver sección Anexo - La plataforma se ajusta a las normas internacionales pertinentes:
4.8	**Formación**			
4.8.1	El oferente deberá presentar un plan de capacitación completo. Este plan debe incluir todos los productos y servicios especificados en su oferta, así como la capacitación del personal encargado de gestionar los equipos, sistemas y componentes que integren la solución propuesta por el oferente. Un curso presencial siempre cada año durante 2 años (2 en total para cada tema). Deberá cubrir todos los aspectos técnicos de la puesta en marcha del proyecto de renovación. Debe incluir todos los productos y servicios incluidos en su oferta. Debe incluir una capacitación al personal que vaya a gestionar las máquinas.	Si	242-259 789-A, 789-E A 789-F 789-I	Ver Sección VII. Capacitación Ver Item Otros Requerimientos. Detalle del Cronograma, punto 8 punto Etapa 3, 12 meses renovable a 10 años. CRONOGRAMA
4.8.2	Para la parte de la Diracion Nacional de Cedulacion, Direccion Ejecutiva del Voto Dominicano en el Exterior y Centros de Expediciones de Actas y Cedulas serian 436 empleados divididos como sigue: 370 local y 66 en el exterior, además de 50 técnicos del equipo de tecnologia. El proveedor adjudicado deberá de capacitar al personal de la JCE (a capacitadores de la JCE, donde será la JCE encargada de capacitar al resto de personal) en la sede central como mínimo, en los siguientes cursos (1 curso por año de cada curso): - Uso, administración y mantenimiento de la PKI - Uso, administración y mantenimiento de las impresoras - Uso, administración y mantenimiento de la cédula digital (app y web) - Uso, administración y mantenimiento de los dispositivos - Uso, administración y mantenimiento de los API's	Si	244 246-247 247-258	Ver Sección VII. Capacitación, punto 1 Plan de Capacitación Punto 4. Temario de Capacitaciones Básicas, 5. Punto 5. Temario de Capacitaciones Avanzadas, 6-18
4.8.2	Áreas a Cubrir en Detalle: Operación y Mantenimiento del Equipo de Impresión: - Instalación y configuración de impresoras de policarbonato. - Procedimientos de personalización de tarjetas. - Mantenimiento preventivo y correctivo de los equipos. Infraestructura de Clave Pública (PKI) y Autoridad de Certificación (CA): - Principios básicos de PKI y su aplicación en documentos de identidad. - Generación, manejo y almacenamiento seguro de claves criptográficas. - Procedimientos para la emisión y revocación de certificados digitales. - Uso y gestión de Módulos de Seguridad por Hardware (HSM). Solución de Mobile ID: - Funcionamiento y uso de la app de Mobile ID desarrollada para la JCE. - Procedimientos de seguridad para la gestión de identidades digitales. - Integración con sistemas existentes y gestión de actualizaciones.	Si	244 246-247 245 245 245 246 246 247 247 247 247-248 248-249	Ver Sección VII. Capacitación, punto 1 Plan de Capacitación Punto 5. Temario de Capacitaciones Avanzadas: 1. Operación y Mantenimiento del Equipo de Impresión, página 4 2. Infraestructura de Clave Pública (PKI) y Autoridad Certificadora (CA), página 4 3. Solución Mobile ID, página 4 4. Temario de Capacitaciones Básicas: 4.1. Capacitación del uso de las impresoras de cédulas, página 5 4.2.Capacitación del mantenimiento básico de la máquina de impresión, página 5 4.3. Introducción de la Cédula Digital. 5. Temario de Capacitaciones Avanzadas: 5.1. Capacitaciones para el uso, Administración y Mantenimiento de la PKI Grabado de Chip, página 6 5.2. Capacitación del uso, administración y mantenimiento de a PKI CA, página 6 5.3. Capacitación para el uso, administración y mantenimiento de impresoras, página 6

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

4.8.3	Niveles de Capacitación: Básico: Capacitación destinada al personal operativo que realizará tareas cotidianas relacionadas con el manejo de los equipos de impresión y las aplicaciones asociadas. Avanzado: Capacitación para el personal técnico y administrativo que supervisará, mantendrá y resolverá problemas complejos relacionados con la infraestructura de PKI, CA, y la solución de Mobile ID.	Si	244 246-259	Ver Sección VII. Capacitación:, punto 1 Plan de Capacitación, página 3 Punto 4. Temario de Capacitaciones Básicas, páginas 246-247 Punto 5. Temario de Capacitaciones Avanzadas, páginas 247-259
5. Kits				
	El total de kits a cotizar y a entregar, serian un (1) kilt. El objetivo de los kits es de reposición de los dispositivos estropeados, dañados u obsoletos, por tanto, será a demanda, en función del criterio de la JCE			
5.1	**Escaner: pueden cumplir con estas características técnicas o superiores, requerido muestra del equipo propuesto.**	Si		
5.1.1	Tipo: Escáner móvil personal.	Si	446	
5.1.2	Alimentación de documentos: Automática o manual.	Si	447	
5.1.3	Color: 24 bits.	Si	447 A	
5.1.4	Fuente de luz: LED RGB.	Si	447 A	
5.1.5	Modos de operación: Color, escala de grises, blanco y negro.	Si	447 A	
5.1.6	Resolución óptica: 600 ppp.	Si	447 A	
5.1.7	Resolución de salida: 150/200/300/400/600 ppp.	Si	447 A	
5.1.8	Velocidades de escaneo: 8 ppm/16 ipm.	Si	447 A	
5.1.9	Interfaz: Hi-Speed USB 2.0.	Si	447 A	
5.10	**Otras caracteristicas:** Detección automática de tamaño de página. Configuración automática de resolución. Suavizamiento de fondo. Corrección de desviación. Énfasis de borde. Reducción del efecto muaré. Corrección de fotografía. Escaneo previo. Eliminación de fondo/prevención de sangrado. Recorte del sombreado. Omisión de página en blanco. Mejoramiento de texto. Reconocimiento de la orientación del texto. Software incluido para Windows: Controladores WIA/TWAIN. Sistemas operativos compatibles: Windows 10, Windows 11.	Si	247	
6	**Lector de firma, Pueden cumplir con estas caracteristicas técnicas o superiores, requerido muestra del equipo propuesto.**	Si	451	
6.1	Dimensiones del producto (aproximadas, similar o superior): 156 x 126 mm.	Si	451	
6.1	Interface de comunicación: USB.	Si	451	
6.1	F-STN, monocromático, reflectante.	Si	451	
6.1	Tamaño de pantalla: +- 4".	Si	451	
6.1	Resolución nativa: a ser propuesta por el licitante	Si	451	
6.1	Niveles de presión del lápiz: 512/1024.	Si	451	
6.1	Resolución del sensor: 2540 líneas por pulgada.	Si	451	
6.1	Bolígrafo sin pilas: Sí.	Si	451	
6.1	Bolígrafo inalámbrico: Sí.	Si	451	
6.1	Velocidad de transmisión (aproximada, similar o superior): 200pps.	Si	451	
7	**Lector de huellas (Compatible con NEUROtechnology, porque la JCE dispone de sistemas y software que usan esta tecnología). Pueden cumplir con estas caracteristicas técnicas o superiores, requerido muestra del equipo propuesto. PUEDE SER DE OTRA MARCA con SDK compatible.**	Si	448	

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

7.1	El lector de huellas requerido se refiere a la modalidad decadactilar, es decir que permita capturar 10 huellas, en formato 4-4-2.	Si	448	
7.2	Tamaño de la ventana de escaneado de huellas dactilares: aproximado de 86 mm x 84 mm.	Si	450	
7.3	Área de escaneo óptico (aproximada, similar o superior): 81 mm x 81 mm.	Si	450	
7.4	Resolución de la imagen (aproximada, similar o superior): 1600 x 1600 píxeles, 500 dpi.	Si	450	
7.5	Profundidad de bit: 8 bit, 256 niveles de gris.	Si	450	
7.6	Tamaño del archivo Raw de la imagen de la huella dactilar comprimido en WSQ aprox. 2,5 MB aproximadas, similar o superior 0,4.	Si	450	
7.7	Interfaz (aproximada, similar o superior): USB 2.0 de alta velocidad con cable USB estándar de alrededor de 1.8 metros.	Si	450	
7.7	Fuente de luz diodos emisores de luz: (LED) infrarroja.	Si	450	
7.8	Fuente de alimentación: Preferiblemente USB.	Si	450	
7.9	Indicar certificaciones.	Si	450	
8	**Lector RFID. 230 lectores de chip sin contacto para control de calidad antes de la entrega la ciudadano. La caracteristicas del lector de tarjetas debe ser Lector para NFC Compatible con ISO 14443 Tipo A, Tipo B y Tarjetas Mifare 1k&4k, ICAO 9303 con interoperabilidad OACI DOC 9303, ISO18013, PA, AA, BAC, EAC , SAC.**	Si	463 a 465	
8	**Impresora termica punto de venta: Pueden cumplir con estas características técnicas o superiores, requerido muestra del equipo propuesto.**	Si	452	
8.1	Dimensiones (aproximadas, similar o superior): 20X20X25.	Si	453	
8.2	Largo del cable (aproximado, similar o superior): 1.8.	Si	453	
8.3	Tipo de inyección: Láser. (Termica)	Si	453	
8.4	Calidad de impresión: Alta resolución.	Si	453	
8.5	Cantidad de puertos USB: 1.	Si	453	
8.6	Tipo de inyección: Láser. (Termica)	Si	453	
8.7	Color: negro.	Si	453	
8.8	Conectividad/conexión y entrada : USB.	Si	453	
8.9	Formato de papel: A7.	Si	453	
8.10	Cantidad de bandejas: 1.	Si	453	
8.11	Velocidad de la impresión a blanco y negro (aproximada, similar o superior): 20.	Si	453	
8.12	Tipo de impresión: Láser monocromática (Termica monocromatica)	Si	453	
9	**Lector de huella digital persona: Pueden cumplir con estas características técnicas o superiores, requerido muestra del equipo propuesto.**	Si	454	
9.1	Voltaje de suministro: 5,0 V ±5 % suministrado mediante USB.	Si	454	
9.2	Corriente de alimentación: escaneo (aproximada, similar o superior) < 100 mA (típico). Corriente de alimentación: en reposo (aproximada, similar o superior) 120 mA (típico). Corriente de alimentación: modo suspensión (aproximada, similar o superior) < 0,5 mA (máximo).	Si	454	
9.3	Inmunidad contra descarga electrostática.	Si	454	
9.4	(ESD, por sus siglas en inglés) >15 kV, montado en la caja.	Si	454	
9.5	Temperatura de operación: 0 - 40 °C.	Si	454	
9.6	Humedad de almacenamiento: 20 % - 90 % sin condensación.	Si	454	
9.7	Información escaneada: Escala de grises de 8 bits.	Si	454	
9.8	Indicar cumplimiento de normas.	Si	454	
9.9	Peso (aproximado, similar o inferior): 105 gramos.	Si	454	
9.10	Interfaz: Dispositivo USB 2.0 de velocidad máxima, de alta potencia	Si	454	
10	**Cámara: Pueden cumplir con estas características técnicas o superiores, requerido muestra del equipo propuesto. Siempre y cuando cumplan con las especificaciones del pliego se aceptan las webcams.**	Si	455	
10.1	Sensor: CMOS.	Si	456	
10.2	Tecnologías: OPCIONAL Wi-Fi® y NFC integradas.	Si	461	
10.3	Sistema de AF de 9 puntos y el modo AF Servo AI.	Si	458	

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R. D.

10.4	Visor óptico con una cobertura del visor de aproximadamente 95% (aproximado, similar o superior).	Si	457	
10.5	Alta definición real (Full HD) de 30p (aproximada, similar o superior).	Si	456	
10.6	Balance automático de blancos con "Prioridad de blancos".	Si	457	
10.7	Puerto USB (para el control del dispositivo/otra tecnología existente para la obtención de la imagen desde una PC).	Si	461	
10.8	Característica de auto enfoque.	Si	458	
10.9	Filtros creativos que incluyen el efecto ojo de pez y el efecto miniatura.	Si	458	
Sección 11 : Cronograma				
11.1	**Etapa 1: Máximo 26 semanas Implantación y puesta en marcha (DEBE CUMPLIR CON TODO LO DESCRITO AQUI ABAJO)** 1.Entregar el diseño de seguridad de las tarjetas a las cuatro (4) semanas después de la firma de contrato. La JCE debe responder en una semana. 2. Suministrar dos impresoras de policarbonato a las dieciséis (16) semanas, así como 2,000 tarjetas genéricas de policarbonato con chip para pruebas. 3. Instalar la PKI y la CA, así como realizar la ceremonia de llaves a las dieciséis (16) semanas. 4. Ayudar a los técnicos de la JCE a adaptar el SDK de la impresora al sistema de la JCE. 5. Realizar pruebas unitarias, de integración, de pre-producción con las impresoras, las tarjetas, personalizando la tarjeta. 6. Realizar las pruebas piloto de la solución digital de la tarjeta CD (Mobile ID) antes de veintiséis (26) semanas, incluyendo el desarrollo de una app para la JCE. 7. Entrega de 300,000 tarjetas de policarbonato a las veintidós (22) semanas después de la firma de contrato. Esta entrega será acompañada con el reporte de laboratorio certificado e independiente, de los test de durabilidad de la tarjeta, así como el chip. 8. Capacitación al personal de la JCE de la operación y mantenimiento del equipo deimpresión, PKI y solución digital.	Si	789-A a 789-C 789G a 789-I	Ver Sección Otros Requerimientos Cronograma Detalle del Cronograma y cronograma, ver etapa 1: Implantación y Puesta en marcha del Proyecto. Página 2 y 3. Finaliza etapa 20 semanas
11.2	**Etapa 2: Máximo 12 meses a partir del fin de la etapa 1. Re-cedulación total de la población (DEBE CUMPLIR CON TODO LO DESCRITO AQUI ABAJO)** el oferente adjudicado tendrá que realizar las siguientes actividades o entregar los siguientes elementos: 1. 500,000 tarjetas de policarbonato a las 26 semanas después de la firma de contrato. 2. 1,200,000 tarjetas de policarbonato a las 30 semanas después de la firma de contrato. 3. 1,000,000 tarjetas de policarbonato a las 34 semanas después de la firma de contrato. 4. 1,000,000 tarjetas de policarbonato a las 38 semanas después de la firma de contrato. 5. 1,000,000 tarjetas de policarbonato a las 42 semanas después de la firma de contrato. 6. 1,000,000 tarjetas de policarbonato a las 46 semanas después de la firma de contrato. 7. 1,000,000 tarjetas de policarbonato a las 50 semanas después de la firma de contrato. 8. 1,000,000 tarjetas de policarbonato a las 54 semanas después de la firma de contrato. 9. Adquisición e instalación de los equipos de impresión y puesta en marcha en las sedes de la República Dominicana y en el exterior. Las fechas de las entregas y cantidades de dichos equipos serán acordados con el proveedor adjudicado y la JCE. 10. Puesta en marcha del mantenimiento de las impresoras en periodo de garantía. Para ello, el proveedor deberá de disponer de mínimo de dos (2) técnicos certificados en tecnología de impresión de tarjetas de identidad, y mínimo un total de diez (10) técnicos para soporte nacional de servicio para reparación de equipos on sitio durante el periodo de garantía. Para el exterior, el proveedor durante tiempo de garantía de las impresoras, deberá reparar en Nueva York (los equipos de Estados Unidos y Canadá) y en Madrid (los equipos de Europa), la JCE enviará las impresoras defectuosas a estos lugares según aplique. 11.ACLARACION IMPORTANTE El sistema de cedulación actual permanece igual. No está incluido en el alcance de esta licitación. Los componentes del concurso deben integrarse a los sistemas actuales, proporcionando el oferente todos los SDK necesarios, los APIS de integración y apoyando en su caso a la Dirección de Informática en su instalación y puesta en marcha. NOTA: La JCE podrá acordar con el adjudicatario el cambio de fechas o de cantidad, por problemas de almacenamiento o de consumo de las tarjetas.	Si	789-C a 789E 789G a 789-I	Ver Sección Otros Requerimientos Cronograma Detalle del Cronograma y cronograma, ver Etapa 2: Máximo 12 meses a partir del fin de la etapa 1. Re-cedulación total de la población, página 3 - 5

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

11.3	**Etapa 3: 12 meses renovable a 10 años. El mantenimiento en todos los casos es solamente por 2 años.** Suministrar tarjetas en la oficina Central de la JCE en base a la demanda que se requiera durante la vigencia del contrato que se estima en 1,000,000 de tarjetas al año, siempre un 10% CI. En todo momento la responsabilidad de poseer disponibilidad de CIs y CIEs es del proveedor. 2. Proveer mantenimiento de los equipos de impresión mientras los equipos estén en garantía. Cuando termine la garantía, los equipos deberán ser atendidos en las siguientes localidades: Para los centros de cedulación ubicados en todo el territorio nacional, serán atendidos en la sede central de la JCE. Para las oficinas OSE ubicadas en Estados Unidos de Norte América, serán atendidas en la OSÉ de New York. Para las oficinas OSE ubicadas en Europa, serán atendidas en la OSE de Madrid. Para las demás oficinas ubicadas en otras demarcaciones, serán atendidas en la Sede Central de la JCE. 3. Proveer mantenimiento de nivel 3 para el mantenimiento del sistema y equipos PKI, y sistemas y equipos para la tarjeta digital.	Si	789-E a 789-F 789-I	Ver Sección Otros Requerimientos Cronograma Detalle del Cronograma y cronograma, ver EEtapa 3: 12 meses renovable a 10 años, página 5

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

AUTO-EVALUACIÓN				
Evaluador:				
Numero de proceso:				
Fecha de evaluación:				
PLANTILLA DE EVALUACIÓN	**PUNTOS MAXIMOS**	**CRITERIOS**	**PUNTOS OBTENIDOS**	**COMENTARIOS DEL OFERENTE**
		FINANCIERO	**7**	
FINANCIERO: 10 PUNTOS	5	**Solvencia: 5 puntos.** Solvencia total (Activo total/Pasivo total) >1,2: **2 puntos.**	2	PROPUESTA LEGAL Y FINANCIERA. REFERIRSE A LOS ESTADOS FINANCIEROS APORTADOS.
		Solidez crediticia: El oferente debe presentar cartas de referencias bancarias y/o entidades financieras, dirigidas a la Junta Central Electoral, que demuestren solvencia y respaldo económico y/o que certifiquen que posee línea de crédito que pueda solventar al menos el monto de USD$2,000,000.00 (o su equivalente en pesos o euros). Para acreditar la solidez, puede ser entre los miembros del consorcio en su conjunto o de forma individual: **3 puntos. Se acepta que al menos uno (1) de los miembros que componen el grupo del consorcio cumpla con este requisito**	3	PROPUESTA LEGAL Y FINANCIERA, Pgs. 204-208. "CARTAS REFERENCIAS BANCARIAS"
	5	**Facturación: 5 puntos.** Consorcio (El total de la facturación debe ser la sumatoria de las empresas que componen el consorcio) factura de media en los últimos 3 años en su conjunto al menos 2 veces más que la totalidad del presupuesto de su propuesta: **3 puntos.**	3	PROPUESTA LEGAL Y FINANCIERA, Pgs. 1138-1139. "REQUISITOS FINANCIEROS - FACTURACION"
		Oferente local factura de media en los 3 últimos años más de USD$5,000,000.00: **2 puntos**	2	PROPUESTA LEGAL Y FINANCIERA, Pgs. 1138-1139. "REQUISITOS FINANCIEROS - FACTURACION"

PLANTILLA DE EVALUACIÓN	PUNTOS MAXIMOS	Criterios	PUNTOS OBTENIDOS	COMENTARIOS DEL OFERENTE
		TECNICA	**20**	
PROPUESTA TÉCNICA: 30 PUNTOS	5	**Menor tiempo para iniciar el proyecto: 5 puntos.** – Hasta 6 meses después de la firma del contrato: **0 puntos.**	2	
		– Hasta 5 meses después de la firma del contrato: **2 puntos.**		PROPUESTA TECNICA, Pag. 789 ("DETALLE DEL CRONOGRAMA DE CUMPLIMIENTO", PUNTO 6, SEMANA 20), PAG. 789I ("CRONOGRAMA").
		– 4,5 meses después de la firma del contrato: **5 puntos.**		
	4	– El oferente presta directamente (sin contratar a terceros) los servicios de desarrollador de PKI, fabricante de tarjetas electrónicas y proveedor de servicios: **2 puntos. El oferente debe ser fabricante de la PKI y fabricante de los sistemas para la generación de la firma del ciudadano para obtener la puntuación completa**	2	PROPUESTA TECNICA, REFIERASE A LA SECCION DE CARTAS JURADAS, SOBRE A DE DOCUMENTOS TECNICOS.
		– El fabricante de las tarjetas y el fabricante de las impresoras, ambos están en la empresa conjunta: **2 puntos.**	2	CONFIRMAMOS QUE CUMPLIMOS CON ESTE PUNTO POR MEDIO A LA EMPRESA MHULBAUER, LA CUAL ES PARTE DELCONSORCIO Y FABRICA TARJETAS E IMPRESORAS.
	5	**Impresoras: 5 puntos.** – Pesa menos de 40 kg.: **3 puntos.**	0	
		– Mide menos de 0,5 m2 (largo x ancho): **1 punto.**	1	PROPUESTA TECNICA, Pg. 464-17. "Ficha Tecnica CLP60", 2.Dimensiones
		– Pueden incorporar un módulo adicional para personalizar la fotografía en color, sin dependencia del policarbonato: **1 punto.**	1	PROPUESTA TECNICA, Pg. 464-15. "Sistema de Personalizacion de Tarjeta", (Productividad/Unidades de Proceso/Caracteristicas).
		Producción de tarjetas: 4 puntos. – El oferente tiene al menos una instalación de producción de respaldo propia para la fabricación de tarjetas en una ubicación distinta de la fábrica principal propuesta de la empresa o la empresa conjunta: **1 punto.**	4	PROPUESTA TECNICA, Pgs. 3-4, ITEM I: "PROPUESTA ESPECIFICACIONES TECNICAS DE LA TARJETA", "CENTRO DE PRODUCCION PRINCIPAL Y CENTRO DE PRODUCCION DE RESERVA".

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, RD

	4	– La construcción del cuerpo de la tarjeta está diseñada sin capas/materiales patentados que limitarían el abastecimiento de materiales de producción de tarjetas a proveedores dedicados: **1 punto.**	1	PROPUESTA TECNICA, Pgs. 7, ITEM I: "PROPUESTA ESPECIFICACIONES TECNICAS DE LA TARJETA", 1.1 "CARACTERISTICAS GENERALES-CONSTRUCCION DE TARJETAS"
		– El cuerpo de la tarjeta en blanco y el proceso de personalización de la misma en combinación no constituirán una solución dependiente o patentada que excluya a los proveedores de tarjetas y/o sistemas de personalización: **2 puntos.**	2	PROPUESTA TECNICA, Pgs. 7, ITEM I: "PROPUESTA ESPECIFICACIONES TECNICAS DE LA TARJETA", 1.1 "CARACTERISTICAS GENERALES-CONSTRUCCION DE TARJETAS"
	8	**Prueba de concepto: 8 puntos.** El proveedor ha realizado una prueba de concepto satisfactoria (realizar una captura de una persona, impresión en láser de la tarjeta de policarbonato, conforme a las especificaciones técnicas de la impresión, de la persona enrolada y luego una generación de una cédula electrónica a partir de esta cédula personalizada). Deberá incluir en dicha prueba, una aplicación móvil de verificación (mediante QR seguro generado desde la aplicación) y mostrar la funcionalidad de compartir un grupo de datos específicos seleccionados por el ciudadano.	8	POR DETERMINARSE
	4	**Diseño gráfico: 4 puntos.** El oferente ha entregado un diseño de seguridad en tres luces (luz visible, luz ultravioleta y luz infrarroja), de la tarjeta electrónica conforme a las bases técnicas en formato imagen de alta resolución.	4	PROPUESTA TECNICA, Pgs. 8-19, ITEM I: "PROPUESTA ESPECIFICACIONES TECNICAS DE LA TARJETA", 1.3 "PROPUESTA DE DISEÑO-CIE&CI"

PLANTILLA DE EVALUACIÓN	PUNTOS MAXIMOS	Criterios	PUNTOS OBTENIDOS	COMENTARIOS DEL OFERENTE
		PROYECTO	5	
PROYECTO: 15 PUNTOS	9	**Plan del proyecto: 9 puntos.** – El proveedor del desarrollo de la cédula digital tiene CMMI DEV 5, o personal implicado en el desarrollo con certificación SIX SIGMA MASTER BLACK BELT o personal implicado en el desarrollo con certificación SAFe 5 o superior de AGILE: **2 puntos.**	2	PROPUESTA TECNICA, Pgs. 499-512, "CURRICULUMS DEL JEFE DE PROYECTOS", CV David Vargas.
		– Si el proveedor aumenta a 5 años la garantía de las impresoras, dando el soporte en sitio del mantenimiento de las impresoras y no en la sede central de la JCE, manteniendo los mismos niveles de acuerdo de servicio: **3 puntos.**	0	
		–El proveedor presenta la implementación, de por lo menos, un desarrollo de una solución , puesta en producción, de cédula digital, en una institución pública, de acuerdo a los requerimientos establecidos en el documento de especificaciones técnicas, y estar adheridas al estándar ISO 18013-5: **4 puntos.**	4	PROPUESTA TECNICA, Pgs. 846-849, "EXPERIENCIA EN DISTINTOS CLIENTES Y PAISES, EN CEDULA DIGITAL O IDENTIDADES MOVILES (MOBILE ID)", E40
	6	**Personal: 6 puntos.** – El oferente contará con un mínimo 2 técnicos certificados en tecnología de impresión de tarjetas de identidad localmente durante la vigencia del contrato para supervisión de la calidad de la e la impresión en todos los centros de impresión de cédulas: **3 puntos.**	6	PROPUESTA TECNICA, Pgs. 482-496, "CURRICULUMS DEL PERSONAL TECNICO CERTIFICADO EN TECNOLOGIAS DE IMPRESION DE TARJETAS DE IDENTIDAD" CVs Yorlin Reyes y Paula Castillo.
		– El oferente contará con un equipo de técnicos (al menos 10) en campo (a nivel nacional) con experiencia en la producción de documentos de identidad nacionales mediante modelo descentralizado de impresión, ofreciendo servicios de instalación, soporte y mantenimiento a la infraestructura de impresión durante los años de garantía de los equipos: **3 puntos.**	3	PROPUESTA TECNICA, Pgs. 499-585, "CURRICULUMS DEL PERSONAL TECNICO EN CAMPO CON EXPERIENCIA EN LA PRODUCCION DE DOCUMENTOS DE IDENTIDAD NACIONALES" (10 CVs)

PLANTILLA DE EVALUACIÓN	PUNTOS MAXIMOS	Criterios	PUNTOS OBTENIDOS	COMENTARIOS DEL OFERENTE
		EXPERIENCIA	3	

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

EXPERIENCIA: 15 PUNTOS	9	Al menos dos (2) experiencias en dos proyectos, de clientes y paises distintos, en el cual el oferente haya llevado a cabo el suministro de impresoras, la instalación, las pruebas, la puesta en servicio y el mantenimiento de un sistema de documentos de identidad electrónicas de policarbonato distribuidas, con impresoras láser en los últimos cinco (5) años, a nivel de gobierno: **3 puntos.**	3	PROPUESTA TECNICA, Pgs. 803-810, "EXPERIENCIA EN PROYECTOS DE DE TARJETAS DE IDENTIDAD ELECTRONICA DE POLICARBONATO", Carta Ministerio de Gobernacion y Policia de Costa Rica, Carta Registro Nacional de Las Personas de Guatemala.
		– Al menos dos (2) experiencias en dos proyectos, de clientes y paises distintos, en los que el licitante haya llevado a cabo un suministro de documentos de identidad electrónicas de policarbonato: **3 puntos.**	3	PROPUESTA TECNICA, Pgs. 810-836, "EXPERIENCIA EN UN PROYECTO DE SUMINISTRO DE TARJETAS DE IDENTIDAD ELECTRONICA DE POLICARBONATO DE TRANSICION DE DOCUMENTOS DE IDENTIFICACION MECANICOS (SIN ELECTRONICA) A DOCUMENTOS D EIDENTIFICACION ELECTRONICA", Carta Ministerio de Gobernacion y Policia de Costa Rica, Carta Ministerio de Interior de Republica de Mozambique, Carta Ministerio del Interior y Comunidades Territoriales.
		– Más de una (1) experiencia, en distintos clientes y paises en proyectos de transición de documentos de identificación sin electrónica a documentos de identificación electrónica. Solo serán válidos contratos de al menos proyectos de 1,000,000 de documentos de identificación al año, dentro de los últimos 5 años a partir de la fecha de presentación de la propuesta: **- 2 contratos: 2 puntos.** **- Más de 2 contratos: 3 puntos.**	3	PROPUESTA TECNICA, Pgs. 804-809, "EXPERIENCIA EN UN PROYECTO DE SUMINISTRO DE TARJETAS DE IDENTIDAD ELECTRONICA DE POLICARBONATO", Carta Ministerio de Gobernacion y Policia de Costa Rica, Carta Registro Nacional de Las Personas de Guatemala.
	3	– Experiencia (acreditable con contratos celebrados con empresas miembros de un mismo grupo económico (empresas con accionistas en común) de los consorciados en distintos clientes y paises, en cédulas digital o identidades móviles (Mobile ID). Solo serán válidos contratos de al menos proyectos de 100,000 cédulas en total, dentro de los últimos 5 años a partir de la fecha de presentación de la propuesta:		
		- 1 contratos: 1 punto.	1	PROPUESTA TECNICA, Pgs. 845-848, "EXPERIENCIA EN DISTINTOS CLIENTES Y PAISES EN CEDULA DIGITAL E IDENTIDADES MOVILES (MOBILE ID)", CARTA REGISTRO NACIONAL DE LAS PERSONAS NATURALES (REP. DE EL SALVADOR).
		- 2 contratos: 2 puntos.		
		- Más de 2 contratos: 3 puntos.		
	1	– Al menos una (1) experiencia, de haber operado un proyecto de impresión de soluciones de identificación a nivel gobierno con el suministro y mantenimiento de al menos 200 impresoras distribuidas nacional o internacional (fuera del país): **1 punto.**	1	PROPUESTA TECNICA, Pgs. 849-851, "EXPERIENCIA DE HABER OPERADO UN PROYECTO DE IMPRESIÓN DE SOLUCIONES DE IDENTIFICACIÓN A NIVEL GOBIERNO CON EL SUMINISTRO Y MANTENIMIENTO DE AL MENOS 200 IMPRESORAS DISTRIBUIDAS NACIONAL O INTERNACIONAL (FUERA DEL PAÍS)". Carta de Real Casa de La Moneda, Fabrica Nacional de Moneda y Timbre.
	2	– Al menos una (1) experiencia, en República Dominicana, en proyectos de mantenimiento de tecnología en gobierno con al menos 5 años de experiencia: **2 puntos.**	2	PROPUESTA TECNICA, Pgs. 849-851, "EXPERIENCIA, EN REPÚBLICA DOMINICANA, EN PROYECTOS DE MANTENIMIENTO DE TECNOLOGÍA EN GOBIERNO CON AL MENOS 5 AÑOS DE EXPERIENCIA", Cartas varias.

PLANTILLA DE EVALUACIÓN	PUNTOS MAXIMOS	Criterios	PUNTOS OBTENIDOS
OFERTA ECONOMICA: 30	30	OFERTA DE MENOR COSTO	0

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.